Chapter 14
Primitive Roots

In this chapter we introduce the concepts of *order* and the *primitive root*, two of the more fascinating and useful ideas in number theory. On the fundamental side, they helped the young Gauss to reduce the equation $x^{16}+x^{15}+\ldots+x+1=0$ to several quadratic equations leading to the construction of the regular 17-gon. These same concepts also allow us to see why the decimal fraction of $1/7$ has a period of length 6, while the decimal fraction for $1/11$ has a period of only 2. And why does $1/99007599$, written as a binary fraction, have a period of nearly 50 million 0's and 1's? We shall see!

Closely related to the primitive root is the concept of *index*, a kind of number-theoretic logarithm that permits us to solve exponential Diophantine equations and even show that $2^n = 3^m - 1$ has only two, and precisely two solutions ($n = 1$, $m = 1$ and $n = 3$, $m = 2$).

Periodic sequences constructed from primitive roots also have an interesting Fourier-transform property that permits the construction of wave-scattering surfaces with very broad scatter and little specular reflection. Such surfaces can be useful in improving concert hall acoustics, in noise abatement measures, and in making ships and planes more difficult to see by sonar or radar. And, of course, there are applications to our main theme: digital encryption and electronic contracting (Sect. 20.3).

14.1 Orders

Some of the things we want to accomplish by electronic mail – other than public key encryption and certified signatures – have to do with certifiable "coin tossing", *registered mail* with or without *receipt*, and *signed contracts*. For these options we need the number-theoretic concepts of a *primitive root* and a *quadratic residue*, both delightful entities in their own right.

Let us look at increasing powers of 2 modulo 7:

$n=1$	2	3	4	5	6
$2^n \equiv 2$	4	1	2	4	1

etc.

M. Schroeder, *Number Theory in Science and Communication*, 5th ed.,
DOI 10.1007/978-3-540-85298-8_14, © Springer-Verlag Berlin Heidelberg 2009

Here the period after which the sequence repeats for the first time is obviously 3. One therefore says that the integer 2 has *order* 3 modulo 7:

$$\mathrm{ord}_7 2 = 3. \tag{14.1}$$

Of course, the order of any integer must be divisor of $p-1$, where p is the prime modulus (7 in our example). This is so because of Fermat's theorem, which requires of any integer b coprime to the modulus p that the congruence $b^{p-1} \equiv 1 \pmod{p}$ must hold. Obviously, for $p=7$, the order could never be 4, for example, because then the sequence of powers would repeat after 4 and 8 steps, etc., and not, as required by Fermat, after $p-1=6$ steps.

What is the largest order of any integer modulo a prime p? Certainly it cannot be larger than $p-1$, because there are only $p-1$ values of least positive residues such that $(m,p)=1$, and once all residues have appeared they *must* repeat.

What is the order of 3 modulo 7? The following table will tell us.

$n =$	1	2	3	4	5	6	7	8
$3^n \equiv$	3	2	6	4	5	1	3	2

etc.

Thus, the order of 3 modulo 7 is 6, the highest possible value. Therefore 3 is called a *primitive root* modulo 7. A primitive root is also called a generating element, or generator, because it generates a complete residue system (in our example the integers from 1 to 6) in some permutation.

Once we have found a primitive root g, we can immediately find another one, its inverse modulo p:

$$g_2 \equiv g_1^{\phi(p)-1} \pmod{p}, \tag{14.2}$$

or, since $\phi(p) = p-1$ for a prime,

$$g_2 \equiv g_1^{p-2}. \tag{14.3}$$

In our example, with $g_1 = 3$, we get $g_2 \equiv 3^5 = 243 \equiv 5 \pmod{7}$. Check: $5 \cdot 3 = 15 \equiv 1 \pmod{7}$. Check! And 5 raised to successive powers yields

$n =$	1	2	3	4	5	6	7	8
$5^n \equiv$	5	4	6	2	3	1	5	4

etc.

Thus 5, too, has order $p-1=6$ and is therefore another primitive root.

How many primitive roots are there? If we raise a given primitive root g to the power $m>1$, where $(m,\phi(p))=1$, then g^m must be another primitive root. Thus there are $\phi(\phi(p))$ primitive roots. (For $p=7$, the number is $\phi(6)=2$, both of which we have already found: 3 and 5.)

If, by contrast, the greatest common divisor (GCD) d of m and $\phi(p)$ is greater than 1, $(m,\phi(p)) = d > 1$, then the order of $g = g_1^m$ is only $\phi(p)/d$. To show this, we observe first that $\phi(p)/d$ is a period of g:

$$g^{\phi(p)/d} = g_1^{\phi(p)m/d} \equiv 1^{m/d} = 1 \pmod{p}, \tag{14.4}$$

and second that it is the *shortest* period, because by introducing the least common multiple $[\phi(p), m]$, we can write

$$g^{\phi(p)/d} = g_1^{[\phi(p),m]} = g_1^{\phi(p)\cdot k} \equiv 1^k = 1 \pmod{p}. \tag{14.5}$$

Thus, $\phi(p)/d$ is the smallest exponent for which $g^{\phi(p)/d}$ is congruent 1 modulo p.

How many positive $m < p$ are there that have order $T = \phi(p)/d$? As we saw in Chap. 7, there are exactly $\phi[\phi(p)/d]$ values of m that have d as the GCD with $\phi(d)$. Hence, the number of residue classes that have order T equals $\phi(T)$. This is illustrated by the following table for $p = 7$, $\phi(p) = 6$:

m	m^2	m^3	m^4	m^5	m^6	T
1	1	1	1	1	1	1
2	4	1	2	4	1	3
3	2	6	4	5	1	6
4	2	1	4	2	1	3
5	4	6	2	3	1	6
6	1	6	1	6	1	2

Indeed, there are exactly $\phi(1) = 1$ order $T = 1$, $\phi(2) = 1$ order $T = 2$, $\phi(3) = 2$ orders $T = 3$ and $\phi(6) = 2$ orders $T = 6$. Further, all T divide $\phi(7) = 6$.

Primitive roots are possessed by the integers 1, 2, 4, p^k and $2 \cdot p^k$ (where p is an *odd* prime and $k > 0$). All that has been said about primitive roots for a prime modulus transfers, *mutatis mutandi*, to these other cases.

The smallest integer not having a primitive root is 8. A prime residue system modulo 8 is given by 1, 3, 5, and 7, and all of these have order 1 or 2: $1^1 \equiv 3^2 \equiv 5^2 \equiv 7^2 \equiv 1 \pmod{8}$. There is no residue that has order $\phi(8) = 4$.

Why are 3 and 5 primitive roots modulo 7 and not, say, 4? How are the primitive roots distributed within a residue system? For example, 71 and 73 both have 24 primitive roots, of which they share exactly one half, namely

11, 13, 28, 31, 33, 42, 44, 47, 53, 59, 62, 68.

What distinguishes these numbers?

Gauss said in his *Disquisitiones* [14.1] that the distribution of primitive roots is a deep mystery; there is no way to predict where they will occur – only their total number is known. But Gauss *did* give some fast algorithms for ferreting them out.

14.2 Periods of Decimal and Binary Fractions

As every high-school student knows, $1/2$ written as a decimal fraction is 0.5 and $1/50$ becomes 0.02. Both 0.5 and 0.02 are *terminating* decimal fractions. By contrast $1/3$ becomes a nonterminating decimal fraction, namely $0.3333\ldots$, and so does $1/7$:

$$0.142857142857\ldots.$$

Both $1/3$ and $1/7$ lead to *periodic* decimal fractions. By contrast $\sqrt{2} = 1.41421356\ldots$ and $\pi = 3.14159265\ldots$ are irrational and have nonterminating aperiodic decimal representation.

What reduced rational fractions m/n, where $(m,n) = 1$, have terminating decimal representation? The answer is very simple and devolves directly from the prime factor decomposition of the denominator n:

$$n = \prod_{p_i|n} p_i^{e_i}, \tag{14.6}$$

where the product is over all prime p_i that divide n. Now, if the only p_i in (14.6) are 2 and 5, then the fraction terminates because 2 and 5 are the only prime factors of 10.

Specifically, if $n = 2^a 5^b$ and, for example, $a > b$, then $n = 2^{a-b}10^b$ and for $a - b = 2$, say,

$$\frac{1}{n} = 0.0\ldots025,$$

where the number of zeros to the right of the decimal point equals b.

Example: $n = 80 = 2^4 \cdot 5 = 2^3 \cdot 10$. Thus, $1/80 = 2^{-3} \times 10^{-1} = 0.0125$.

The numerator m of the fraction m/n simply converts a terminating decimal fraction into another terminating decimal fraction.

Things become more interesting if the denominator n is divisible by prime factors other than 2 or 5. Let us begin with the prime factor 3 and write

$$\frac{1}{3} = \frac{3}{9} = \frac{3}{10-1} = \frac{3}{10} \cdot \frac{1}{1 - \frac{1}{10}} = \frac{3}{10} \cdot \left[1 + \frac{1}{10} + \frac{1}{100} \ldots\right].$$

This brings the periodic nature of the decimal fraction for $1/3$ into direct evidence. The fraction $3/10$ is, of course, 0.3 and the 3 has to be repeated over and over again with increasing right shifts:

$$\frac{1}{3} = 0.3 + 0.03 + 0.003 + \ldots = 0.333\ldots.$$

To save ink, periodic decimal fractions are usually written with a bar over a single period. Thus, $1/3 = 0.\overline{3}$ and $1/7 = 0.\overline{142857}$.

But why does $1/7$ have a period length of 6? Modeling $1/7$ on what we did to $1/3$, we might try to express $1/7$ as a rational fraction with a denominator that is one less than a power of 10. Thus, we are looking for the smallest positive factor f such that

$$7f = 10^k - 1, \tag{14.7}$$

or, equivalently, we want to know the smallest k for which

$$10^k \equiv 1 \pmod{7}. \tag{14.8}$$

That is, of course, just the definition of *order* (in the arithmetic sense!) that we encountered in Sect. 14.1. Thus,

$$k = \operatorname{ord}_7 10 = 6. \tag{14.9}$$

Check: $10^6 = 142857 \cdot 7 + 1$, and no lower power of 10 exceeds a multiple of 7 by 1. Check!

Hence, $1/7$ has a decimal period of length 6 with the digits

$$f = \frac{10^6 - 1}{7} = 142857, \quad \text{or} \tag{14.10}$$
$$\frac{1}{7} = 0.\overline{142857}.$$

More generally, $1/p$, $p \neq 2$ or 5, has a period length

$$k = \operatorname{ord}_p 10. \tag{14.11}$$

Example: For $p = 11$, $k = 2$, $f = 99/11 = 9$; hence $1/11 = 0.\overline{09}$. For $p = 13$, $k = 6$, $f = 999999/13 = 76923$; hence $1/13 = 0.\overline{076923}$.

It is also clear that the period cannot be longer than $p - 1$, because in carrying out the long division $1/p$, there are at most $p - 1$ possible remainders, namely $1, 2, \ldots, p - 1$, after which the remainders and therefore also the decimal digits *must* repeat.

In fact, $\operatorname{ord}_p 10$ is always less than p, because according to Fermat's theorem, for $(p, 10) = 1$:

$$10^{p-1} \equiv 1 \pmod{p}. \tag{14.12}$$

Thus $\operatorname{ord}_p 10$ is either $p - 1$ (as in the case of $p = 7$) or a proper divisor of $p - 1$ (as in the cases $p = 11$ and $p = 13$).

The longest possible period $p - 1$ occurs whenever 10 is a primitive root of p. According to *Abramowitz* and *Stegun* [14.2], 10 is a primitive root of $p = 7$, 17, 19, 23, 29, 47, 59, 61, 97, etc.

Example: $\frac{1}{17} = 0.\overline{0588235294117647}$, which indeed has period length 16.

Of course, pocket calculators are not accurate enough to determine the 96 digits of the decimal period of $1/97$ directly. However, there is a trick that allows us to get the desired digits nevertheless. We shall illustrate this with the 16 digits of the period of $1/17$. A 10-digit pocket calculator shows that

$$\frac{100}{17} = 5.88235294(1),$$

where the last digit may have been rounded off and is therefore uncertain. We have thus found 9 of the 16 digits. The next digits are obtained by calculating, say,

$$\frac{160}{17} = 9.41176470(6).$$

Thus we have found all 16 digits of $1/17$. By merging the two digit strings we obtain

$$\frac{1}{17} = 0.\overline{0588235294117647}.$$

We leave it to the reader to discover a general and efficient algorithm for generating the digits of periodic fractions with a calculator of limited accuracy. In [14.3] all primes with period lengths less than 17 are listed. Surprisingly, 37 is the only prime with period length 3.

Without derivation or proof we also state that for

$$n = \prod_{p_i \neq 2,5} p_i^{n_i}, \tag{14.13}$$

the decimal expression has a period length T equal to the least common multiple of the orders of 10 with respect to the different p_i. Thus, with

$$k_i := \text{ord}_{p_i^{n_i}} 10, \tag{14.14}$$

$$T = [k_1, k_2, \ldots]. \tag{14.15}$$

Proving this is a nice exercise. If n also contains factors 2 or 5, the decimal fractions are mixed, meaning they have a nonperiodic “head”.

Example: $1/119 = 1/(7 \cdot 17)$ has period length $T = [6, 16] = 48$. And for $1/2737 = 1/(7 \cdot 17 \cdot 23)$, $T = [6, 16, 22] = 528$.

Nonunitary fractions have a cyclically shifted period with respect to the corresponding unitary fractions, provided $T = \phi(n)$. Otherwise there are $\phi(n)/T$ different cycles, all of length T.

Example: $1/7 = 0.\overline{142857}$ and $6/7 = 0.\overline{857142}$. But for 13 we have $\phi(13) = 12$ and $\text{ord}_{13} 10 = 6$; thus there are $12/6 = 2$ different cycles: $1/13 = 0.\overline{076923}$ and $2/13 = 0.\overline{153846}$.

Everything that has been said here about decimal fractions carries over to other number bases. For example, $1/3$ in binary notation has period length $T = \text{ord}_3 2 = 2$. In fact, $1/3 = 0.\overline{01}$. For $1/5$ in binary, $T = \text{ord}_5 2 = 4$, and indeed, $1/5 = 0.\overline{0011}$. The prime 9949 has 2 as a primitive root [14.2]. Therefore, $\text{ord}_{9949} 2 = 9948$ and $1/9949$ will generate a sequence of 0’s and 1’s with period lengths $9948 = 2^2 \cdot 3 \cdot 829$.

Another prime in the same range having 2 as a primitive root is 9851. With $9850 = 2 \cdot 5^2 \cdot 197$, the binary expansion of $1/99007599 = 1/(9949 \cdot 9851)$ has a period length $T = [2^2 \cdot 3 \cdot 829, 2 \cdot 5^2 \cdot 197] = 48993900$. Here is a method of generating long pseudorandom binary sequences! What are their spectral properties?

14.3 A Primitive Proof of Wilson's Theorem

Because the sequence of least positive residues $g^k \pmod p$, $k = 1, 2, \ldots, p-1$ (where g is a primitive root of the prime p), is a permutation of the integers $1, 2, \ldots, p-1$, one has

$$(p-1)! = 1{\cdot}2\ldots(p-1) \equiv g{\cdot}g^2\ldots g^{p-1} = g^{p\frac{p-1}{2}} \equiv g^{\frac{p-1}{2}} \pmod p. \qquad (14.16)$$

Now according to Fermat,

$$g^{p-1} \equiv 1 \pmod p. \qquad (14.17)$$

Therefore

$$g^{\frac{p-1}{2}} \equiv \pm 1 \pmod p. \qquad (14.18)$$

However the plus sign is impossible, because g is a primitive root and $p-1$ is the smallest exponent m for which g^m is congruent to 1. Thus,

$$g^{\frac{p-1}{2}} \equiv -1 \pmod p, \qquad \text{i.e.,} \qquad (14.19)$$

$$(p-1)! \equiv -1 \pmod p, \qquad (14.20)$$

which is Wilson's theorem. (However, note that we had to assume the *existence* of a primitive root!)

14.4 The Index – A Number-Theoretic Logarithm

Let m have the primitive root g. For the prime residue system $(k, m) = 1$, one defines the *index* of k modulo m as the smallest positive t for which

$$g^t \equiv k \pmod m, \qquad (14.21)$$

and writes

$$t = \operatorname{ind}_g k.$$

Read: t equals the index to the base g of k.

Example: for $m = 5$ and $g = 2$:

$$\operatorname{ind}_2 1 = 0, \quad \operatorname{ind}_2 2 = 1, \quad \operatorname{ind}_2 3 = 3, \quad \operatorname{ind}_2 4 = 2.$$

It is easy to see that

$$\operatorname{ind}_g(ab) \equiv \operatorname{ind}_g a + \operatorname{ind}_g b \pmod{\phi(m)}, \qquad (14.22)$$

a property the index shares with the logarithm. And in fact, the index is used much like a logarithm in numerical calculations in a prime residue system. For example, the congruence

$$3x \equiv 2 \pmod{5}$$

is converted to

$$\mathrm{ind}_2 3 + \mathrm{ind}_2 x \equiv \mathrm{ind}_2 2 \pmod{4},$$

or with the above “index table”

$$\mathrm{ind}_2 x \equiv 1 - 3 = -2 \equiv 2 \pmod{4}.$$

Thus,

$$x = 4.$$

Check: $3 \cdot 4 = 12 \equiv 2 \pmod{5}$. Check!

A rule that is handy for base conversion is

$$\mathrm{ind}_a b \cdot \mathrm{ind}_b a \equiv 1 \pmod{\phi(m)}, \tag{14.23}$$

which is reminiscent of $\log_a b \cdot \log_b a = 1$ for logarithms.

In preparing index tables, it is only necessary to list values for primes, because index values of composites are obtained by addition. Also, one-half of a complete index table is redundant on account of the following symmetry relation:

$$\mathrm{ind}(m - a) \equiv \mathrm{ind}\, a + \tfrac{1}{2}\phi(m) \pmod{\phi(m)}, \tag{14.24}$$

which is a consequence of

$$g^{\frac{1}{2}\phi(m)} \equiv -1 \pmod{m}. \tag{14.25}$$

14.5 Solution of Exponential Congruences

The exponential congruence

$$a^x \equiv b \pmod{m}, \tag{14.26}$$

if *m* has a primitive root, can be solved by index-taking

$$x \cdot \mathrm{ind}\, a \equiv \mathrm{ind}\, b \pmod{\phi(m)}, \tag{14.27}$$

which has a solution *iff*

$$(\operatorname{ind} a, \phi(m)) \mid \operatorname{ind} b. \tag{14.28}$$

In fact, in that case, there are $(\operatorname{ind} a, \phi(m))$ incongruent solutions.

Example: $7^x \equiv 5 \pmod{17}$; with the primitive root $g = 3$ as a base, we have

$$x \cdot 11 \equiv 5 \pmod{16}.$$

Since $(11, 16) = 1$ divides 5, there is one (and only one) incongruent solution. Using Gauss's recipe,

$$x \equiv \frac{5}{11} \equiv \frac{5}{-5} = -1 \equiv 15 \pmod{16}.$$

Check: $7^{15} = 7^{16}/7 \equiv 1/7 \equiv 5 \pmod{17}$. Check!

In Sect. 7.6 on exponential Diophantine equations we considered the equation

$$2^n = 3^m - 1 \tag{14.29}$$

and asked whether there were solutions other than $2 = 3 - 1$ and $8 = 9 - 1$. Unfortunately, the answer was negative, otherwise we could have used ternary maximum-length sequences for precision measurements whose period was a power of 2, making them amenable to Fast Fourier Transformation (FFT) algorithms.

Now we consider another equation and ask: does

$$3^n = 2^m - 1$$

have any solutions other than $n = 1$, $m = 2$? If so, we could use binary maximum-length sequences whose period is a power of 3, making only slightly less efficient FFT algorithms based on the factor 3 (rather than 2) applicable.

We shall answer the above question using the concept of the *order* of an integer [14.4]. We ask: is there a solution of the above equation for $n > 1$? If there were, then $3^n = 9 \cdot k$ for some integer $k \geq 1$. Thus,

$$2^m \equiv 1 \pmod{9}.$$

Now the order of 2 modulo 9 is 6:

$$\operatorname{ord}_9 2 = 6.$$

Check: $2^r \equiv 2, 4, 8, 7, 5, 1 \pmod{9}$. Check! This means that 6 must divide the exponent m in the above congruence:

$$m = 6b \quad \text{for some integer } b.$$

Hence,

$$2^m = 2^{6b} = (2^3)^{2b} = 8^{2b} \equiv 1^{2b} = 1 \pmod{7}.$$

In other words, 7 divides $2^m - 1 = 3^n$, a contradiction because by the fundamental theorem, 3^n cannot be divisible by 7. Consequently, $n \leq 1$ and $3^1 = 2^2 - 1$ is the only solution. Too bad for our intended application!

In a similar vein [14.4], we prove that there are no solutions to

$$2^a = 3^b - 1 \tag{14.30}$$

for $a > 3$ or $2^a = 16 \cdot k$ for some integer $k \geq 1$. Thus, for $a > 3$:

$$3^b \equiv 1 \pmod{16}.$$

Since $\operatorname{ord}_{16} 3 = 4$, b must be some multiple of 4:

$$b = 4 \cdot r$$

for some integer $r \geq 0$. Thus,

$$3^{4r} \equiv 1 \pmod{16}.$$

Now, note that $\operatorname{ord}_5 3 = 4$, i. e.,

$$3^4 \equiv 1 \pmod{5},$$

and therefore also

$$3^{4r} = 3^b \equiv 1 \pmod{5},$$

or, equivalently,

$$5 | (3^b - 1) = 2^a,$$

a contradiction because 5 cannot divide a power of 2! Thus, $a = 1$, $b = 1$ and $a = 3$, $b = 2$ are the sole solutions of $2^a = 3^b - 1$.

14.6 What is the Order T_m of an Integer m Modulo a Prime p?

As another example of solving exponential congruences we shall consider the congruence

$$m^{T_m} \equiv 1 \pmod{p} \quad \text{or} \tag{14.31}$$

$$T_m \cdot \operatorname{ind} m \equiv 0 \pmod{\phi(p)}, \qquad \text{i. e.,} \tag{14.32}$$

$$T_m \cdot \operatorname{ind} m = k\phi(p). \tag{14.33}$$

Here the left-hand side must be both a multiple of $\phi(p)$ and $\operatorname{ind} m$ and, because of the definition of T_m as the *smallest* solution, $T_m \cdot \operatorname{ind} m$ must be the *least* common multiple $[\operatorname{ind} m, \phi(p)]$:

$$T_m \cdot \operatorname{ind} m = [\operatorname{ind} m, \phi(p)] = \frac{\operatorname{ind} m \cdot \phi(p)}{d}, \tag{14.34}$$

where d is the greatest common divisor of $\operatorname{ind} m$ and $\phi(p)$. Thus,

$$T_m = \frac{\phi(p)}{d}. \tag{14.35}$$

For example, for $p = 7$ and $m = 2$ and using 3 as the index base: $\operatorname{ind}_3 2 = 2$ and $T_2 = 6/(2,6) = 3$, i. e., the order of 2 modulo 7 is 3. Check: $2^3 = 8 \equiv 1 \pmod 7$ and $2^k \not\equiv 1 \pmod 7$ for $k < 3$. Check!

If we had taken 5 as the index base, the answer would have been the same: $\operatorname{ind}_5 2 = 4$ and $T_2 = 6/(4,6) = 3$. Check!

14.7 Index “Encryption”

The public-key encryption method described earlier is based on the fact that exponentiation modulo a large composite number whose factors are not known is apparently a “trap-door function”, i. e., it is easy to exponentiate with a known exponent and to calculate a remainder, but it is very difficult to go in the opposite direction, i. e., to determine which number has to be exponentiated to yield a known remainder.

Another way to describe this situation, for the case that the modulus has a primitive root, is to say that taking logarithms in number theory (i. e., determining an index) is a difficult operation. While the encrypted Message E is given by

$$E \equiv M^s \pmod r, \tag{14.36}$$

the original message M can be obtained, at least formally, by taking the index to the base g, where g is a primitive root of r:

$$\operatorname{ind}_g E \equiv s \cdot \operatorname{ind}_g M \pmod{\phi(r)} \quad \text{or} \tag{14.37}$$

$$M \equiv g^{(\operatorname{ind} E)/s} \pmod r. \tag{14.38}$$

Example: $r = 17$, $g = 3$, $s = 5$. Say the cryptogram is $E = 7$. Then, with

$$\operatorname{ind}_3 7 = 11 \pmod{16} \qquad \text{and}$$
$$\frac{\operatorname{ind} E}{s} = \frac{11}{5} \equiv \frac{-5}{5} = -1 \equiv 15 \pmod{16},$$

the original message is

$$M \equiv 3^{15} \equiv 6 \pmod{17}.$$

Check: $6^5 \equiv 7 \pmod{17}$. Check!

The disadvantage in serious applications of index encryption is that the modulus r is limited to integers that have primitive roots, i. e., primes, odd prime powers and twice odd prime powers (apart from 1, 2 and 4).

14.8 A Fourier Property of Primitive Roots and Concert Hall Acoustics

Consider the sequence

$$a_n = \exp\left(\frac{\mathrm{i}2\pi g^n}{p}\right), \tag{14.39}$$

where g is a primitive root of the prime p. This sequence is periodic, with period $\phi(p) = p-1$. Also, the a_n have magnitude 1.

The *periodic correlation sequence* is defined by

$$c_m := \sum_{n=0}^{p-2} a_n a^*_{n+m}, \tag{14.40}$$

where a^* stands for the complex conjugate of a. Obviously,

$$c_0 = p-1, \tag{14.41}$$

or, more generally, $c_m = p-1$ for $m \equiv 0 \pmod{p-1}$.

On the other hand, for $m \not\equiv 0 \pmod{p-1}$,

$$c_m = \sum_{n=0}^{p-2} \exp\left[\frac{\mathrm{i}2\pi g^n(1-g^m)}{p}\right]. \tag{14.42}$$

Here the factor $1-g^m \not\equiv 0 \pmod{p}$, and $g^n(1-g^m)$ therefore runs through a complete prime residue system except 0 as n goes from 0 to $p-2$. Thus, c_m is the sum over a complete set of pth roots of 1, except 1 itself. Since the "complete" sum equals 0, we have

$$c_m = -1, \quad \text{for } m \not\equiv 0 \pmod{p-1}. \tag{14.43}$$

Now, a periodic correlation function that has only two distinct values ($p-1$ and -1 in our case) has a *power spectrum* with only two distinct values [14.5]. By power spectrum we mean the absolute square of the Discrete Fourier Transform (DFT) defined by

$$A_m := \sum_{n=0}^{p-2} a_n \,\mathrm{e}^{-2\pi \mathrm{i} nm/(p-1)}. \tag{14.44}$$

It is easy to show that the power spectrum is given by

$$|A_m|^2 = \sum_{k=0}^{p-2} c_k \, \mathrm{e}^{-2\pi \mathrm{i} km/(p-1)}, \tag{14.45}$$

i. e., by the DFT of the correlation sequence. This is reminiscent of the well-known Wiener-Khinchin theorem [14.6].

For $m = 0$, or more generally $m \equiv 0 \pmod{p-1}$, we have, with the above two values for c_k,

$$|A_0|^2 = 1. \tag{14.46}$$

For $m \not\equiv 0 \pmod{p-1}$, with $c_0 = p-1$ and $c_k = -1$, we get

$$|A_m|^2 = p - 1 - \sum_{k=1}^{p-2} \mathrm{e}^{-2\pi \mathrm{i} km/(p-1)}, \tag{14.47}$$

where the sum is again over a complete set of roots of 1, except 1 itself. Thus,

$$|A_m|^2 = p \quad \text{for all } m \not\equiv 0 \pmod{p-1}. \tag{14.48}$$

Such a constant power spectrum is called “flat” or “white” (from “white light”, except that white light has a flat spectrum only in the *statistical* sense).

14.9 More Spacious-Sounding Sound

Flat power spectra are important in physics and other fields. (For example, a good loudspeaker is supposed to radiate a flat power spectrum when driven by a short electrical impulse.) Here, in addition, the original sequence a_n, whose spectrum is flat, has constant magnitude 1. This leads to an interesting application in concert hall acoustics.

It has been shown that concert halls with laterally traveling sound waves, all else being equal, have a superior sound [14.7] to those halls that furnish short-path sound arriving only from the front direction – as is the case in many modern halls with low ceilings (dictated by high building costs and made possible by modern air conditioning). To get more sound energy to arrive at the listeners’ ears from the sides (laterally), the author [14.8] proposed scattering, or diffusing, the sound which emanates from the stage and is reflected from the ceiling in all directions except the specular direction [14.9]. Also, the ceiling should not absorb any sound: in a large modern hall every “phonon”, so to speak, is valuable; otherwise the overall sound level (loudness) will be too low.

Thus, what is called for on the ceiling is something the physicist calls a *reflection phase-grating* that scatters equal sound intensities into all diffraction orders except the zero order. Here “order” is used not as defined in mathematics but as in physics. Zero-order diffraction corresponds to the specular direction, i. e., straight downward.

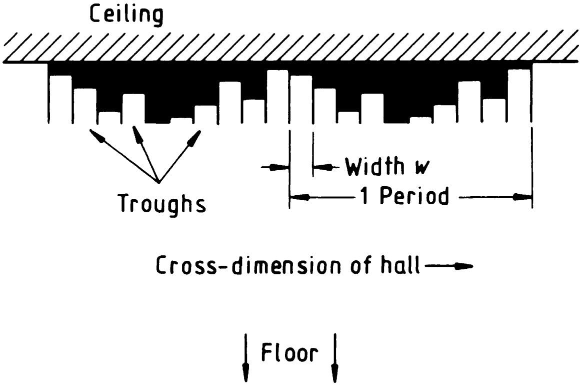

Fig. 14.1 Concert hall ceiling designed as a reflection phase-grating (based on the primitive root 2 of the prime 11)

Reflection phase-gratings can be realized by a hard surface with "wells" of different depths d_n, as shown in Fig. 14.1. Upon reflection, the phase of a normally incident wave is changed by $2d_n 2\pi/\lambda$, where λ is the wavelength. Now, if the depths d_n are chosen according to

$$d_n = \frac{1}{2}\frac{\lambda g^n}{p}, \tag{14.49}$$

where g is a primitive root of the prime p, and g^n can be the least residue modulo p, then the reflected wave has complex amplitudes[1] on its "wavefront" according to

$$a_n = \mathrm{e}^{2\pi \mathrm{i} g^n/p},$$

just like the periodic sequence that we considered above and that had a flat power spectrum.

Now, if the spatial distribution of wave amplitudes along a plane surface has a *flat* power spectrum, then the intensities of the wavelets scattered into the different diffraction orders will all be equal. Hence we expect a ceiling constructed according to this principle, as shown in Fig. 14.1 for $p = 11$ and $g = 2$, to scatter sound widely except in the specular direction (downward). That this is indeed so is illustrated in Fig. 14.2, which shows the result of actual measurements on a "primitive root" ceiling designed for improving concert hall acoustics. Such ceilings can be expected to increase the feeling of spaciousness, i. e., of being surrounded by or "bathed" in sound.

In order to form a *two*-dimensional array that scatters equal intensities into all diffraction orders (except the zeroth) over the *solid* angle, the prime p must be so chosen that $p-1$ has two coprime factors. For example, for $p = 11$, $p-1 = 10 = 2\cdot 5$

[1] This is taking an approximate ("Kirchhoff") view of diffraction. In reality, the complex amplitude cannot change abruptly. For an exact treatment, see [14.10].

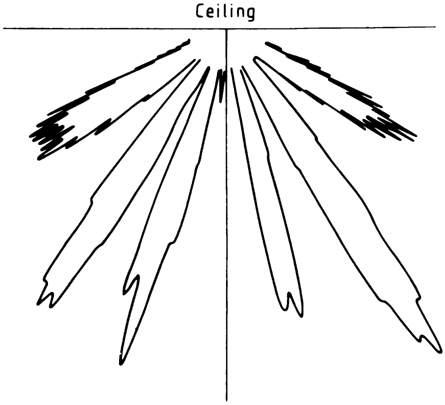

Fig. 14.2 Backscatter from primitive root ceiling. Note low specular reflection (vertically downward). $p = 7$, $g = 3$

and the ten numbers a_n can be used to fill a 2-by-5 array in "Chinese remainder" fashion (Chap. 17), for example as follows:

$$\begin{array}{ccccc} a_1 & a_7 & a_3 & a_9 & a_5 \\ a_6 & a_2 & a_8 & a_4 & a_{10}, \end{array} \tag{14.50}$$

i. e., the horizontal (left-to-right) location of a_n in the array corresponds to $\langle n \rangle_5$ and the vertical (up-down) location of a_n is given by $\langle n \rangle_2$. More generally, the array locations can be given by $\langle k \cdot n \rangle_5$, with any k for which $(k, 5) = 1$, and $\langle m \cdot n \rangle_2$, with $(m, 2) = 1$ (i. e., m must be odd). Here the acute brackets signify least remainders (see Sect. 17.2 on Sino-representation).

In the most general case, an r-dimensional array with the desired r-dimensional correlation and Fourier properties can be formed if $p - 1$ has r pairwise coprime factors $q_1, q_2, \ldots, q_r$ and the location in the array of a_n has the coordinates

$$\langle k_i \cdot n \rangle_{q_i}, \quad \text{with} \quad (k_i, q_i) = 1, \quad i = 1, 2, \ldots, r. \tag{14.51}$$

For three-dimensional arrays, the smallest prime p such that $p - 1$ has three coprime factors is 31. Indeed, $30 = 2 \cdot 3 \cdot 5$, giving a 2-by-3-by-5 array.

Another important principle that can be employed to diffuse sound involves *quadratic residues* (Chap. 16), and an interesting application of primitive roots, to the splicing of telephone cables, is given in [14.11].

14.10 Galois Arrays for X-Ray Astronomy

X-rays are notoriously difficult to focus. For X-ray photons, the index of refraction of most earthly materials is so close to 1 that focussing lenses are all but impossible to construct. This is a pity because the skies abound with interesting emitters of X-rays. Fortunately, X-rays can be easily *blocked* by lead and other materials opaque

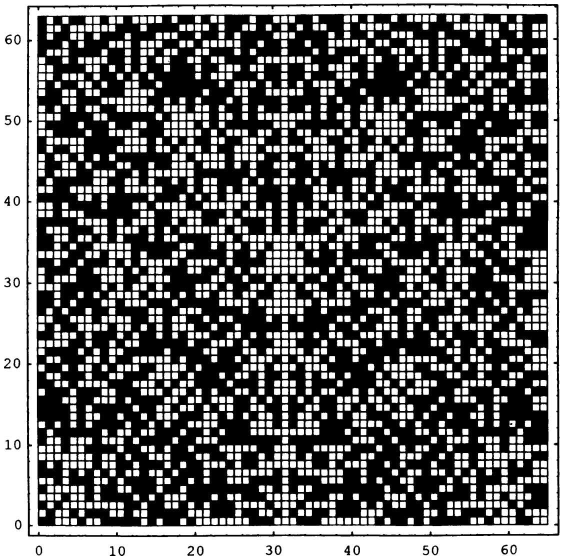

Fig. 14.3 Shadow mask for X-ray astronomy based on Galois sequence of length 4095

to X-rays. The question then is "can we image X-rays sources with the help of partially opaque masks?" And what patterns of opaqueness and translucence must such a "shadow mask" have to form useful images?

One solution is a two-dimensional pattern of opaqueness (0) and translucence (1) obtained from a Galois sequence (see Chap. 28) whose length $L = 2^m - 1$ can be factored into (at least) two coprime factors. For a nearly square-shaped mask, one chooses an even exponent, $m = 2k$, and obtains $L = 2^{2k} - 1 = (2^k + 1)$

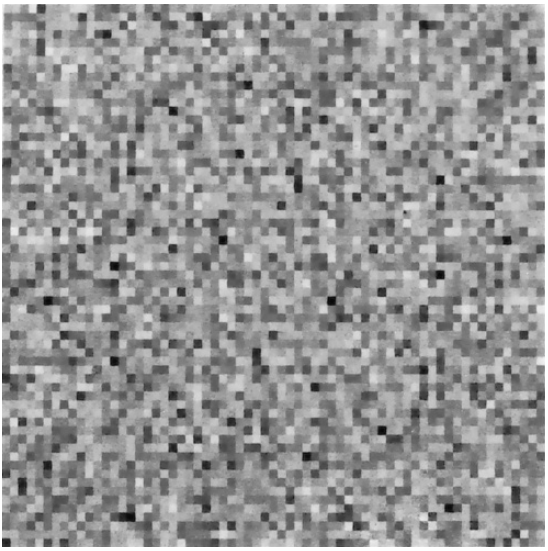

Fig. 14.4 Simulated X-ray shadow obtained with mask shown in Fig. 14.3

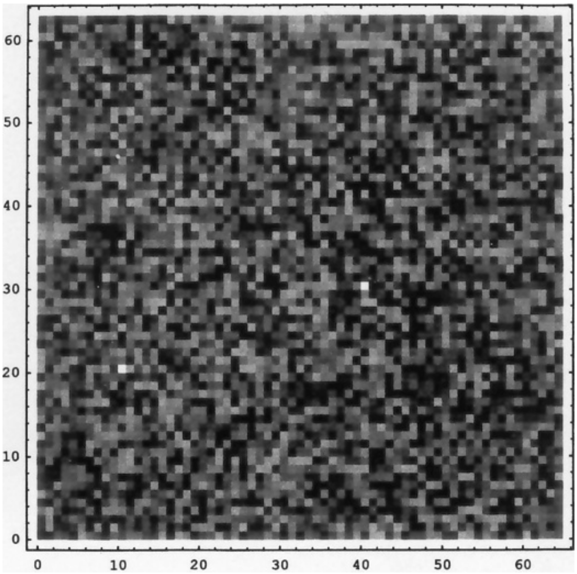

Fig. 14.5 X-ray image obtained by deconvolving data shown in Fig. 14.4. Note the two X-ray sources

$(2^k - 1)$. Figure 14.3 shows such a mask for $m = 12$ with side lengths 63 by 65. Note the bilateral symmetry around the vertical. Interestingly, the rows of length 63 are themselves Galois sequences. All this is no accident but can be proved rigorously, albeit by methods beyond the scope of this book. However, the interested reader might try to derive these results without the use of the relevant number-theoretic concepts (*trace* and *norm*).

Figure 14.4 shows the shadow of two distant X-ray sources cast by such a mask. Observing this data with photon counters and scanning it into a computer allows a reconstruction of the X-ray source by a two-dimensional deconvolution process. Figure 14.5 shows the result of this imaging method for *two* (incoherent) X-ray point sources [14.12].

14.11 A Negative Property of the Fermat Primes

The Fermat primes are, as Gauss discovered, precisely those primes p for which a "Euclidean" construction of the regular p-gon is possible (see Sect. 3.9). Thus, being a Fermat prime makes something possible.

Curiously, being a Fermat prime also makes something *impossible*, namely the construction of two- or higher-dimensional primitive-root arrays, as described in the preceding section. For such arrays, $p - 1$ must be factored into two or more coprime factors, but $p - 1$ has only *one* prime factor, namely 2. Thus, the same circumstance that allows the Euclidean construction forbids the construction of primitive-root arrays with more than one dimension (a form of mathematical justice?).