WIKIPEDIA

Primitive root modulo *n*

In modular arithmetic, a branch of number theory, a number g is a **primitive root modulo n** if every number a coprime to n is congruent to a power of g modulo n. That is, for every integer a coprime to n, there is an integer k such that $g^k \equiv a \pmod{n}$. Such k is called the **index** or **discrete logarithm** of a to the base g modulo n.

In other words, g is a generator of the multiplicative group of integers modulo n.

Gauss defined primitive roots in Article 57 of the Disquisitiones Arithmeticae (1801), where he credited Euler with coining the term. In Article 56 he stated that Lambert and Euler knew of them, but he was the first to rigorously demonstrate that primitive roots exist for a prime n. In fact, the *Disquisitiones* contains two proofs: the one in Article 54 is a nonconstructive existence proof, while the other in Article 55 is constructive.

Contents

Elementary example

The number 3 is a primitive root modulo 7[1] because

$$\begin{aligned}
3^1 &= 3 = 3^0 \times 3 \equiv 1 \times 3 = 3 \equiv 3 \pmod 7 \\
3^2 &= 9 = 3^1 \times 3 \equiv 3 \times 3 = 9 \equiv 2 \pmod 7 \\
3^3 &= 27 = 3^2 \times 3 \equiv 2 \times 3 = 6 \equiv 6 \pmod 7 \\
3^4 &= 81 = 3^3 \times 3 \equiv 6 \times 3 = 18 \equiv 4 \pmod 7 \\
3^5 &= 243 = 3^4 \times 3 \equiv 4 \times 3 = 12 \equiv 5 \pmod 7 \\
3^6 &= 729 = 3^5 \times 3 \equiv 5 \times 3 = 15 \equiv 1 \pmod 7 \\
3^7 &= 2187 = 3^6 \times 3 \equiv 1 \times 3 = 3 \equiv 3 \pmod 7
\end{aligned}$$

Here we see that the period of 3^k modulo 7 is 6. The remainders in the period, which are 3, 2, 6, 4, 5, 1, form a rearrangement of all nonzero remainders modulo 7, implying that 3 is indeed a primitive root modulo 7. This derives from the fact that a sequence (g^k modulo n) always repeats after some value of k, since modulo n produces a finite number of values. If g is a primitive root modulo n, then the period of repetition is n-1. Curiously, permutations created in this way (and their circular shifts) have been shown to be Costas arrays.

Definition

If n is a positive integer, the integers between 0 and n − 1 that are coprime to n (or equivalently, the congruence classes coprime to n) form a group with multiplication modulo n as the operation; it is denoted by $\mathbf{Z}_n^\times$ and is called the group of units modulo n or the group of primitive classes modulo n. As explained in the article multiplicative group of integers modulo n, this group is cyclic if and only if n is equal to 2, 4, p^k, or $2p^k$ where p^k is a power of an odd prime number.[2][3][4] A generator of this cyclic group is called a **primitive root modulo n**,[5] or a **primitive element of $\mathbf{Z}_n^\times$**.

The order of (i.e., the number of elements in) $\mathbf{Z}_n^\times$ is given by Euler's totient function $\varphi(n)$ (sequence A000010 in the OEIS). Euler's theorem says that $a^{\varphi(n)} \equiv 1 \pmod{n}$ for every a coprime to n; the lowest power of a which is congruent to 1 modulo n is called the multiplicative order of a modulo n. In particular, for a to be a primitive root modulo n, $\varphi(n)$ has to be the smallest power of a which is congruent to 1 modulo n.

Examples

For example, if $n = 14$ then the elements of $\mathbf{Z}_n^\times$ are the congruence classes {1, 3, 5, 9, 11, 13}; there are $\varphi(14) = 6$ of them. Here is a table of their powers modulo 14:

```
x     x, x^2, x^3, ... (mod 14)
1 :   1
3 :   3,  9, 13, 11,  5,  1
5 :   5, 11, 13,  9,  3,  1
9 :   9, 11,  1
11 :  11,  9,  1
13 :  13,  1
```

The order of 1 is 1, the orders of 3 and 5 are 6, the orders of 9 and 11 are 3, and the order of 13 is 2. Thus, 3 and 5 are the primitive roots modulo 14.

For a second example let $n = 15$. The elements of $\mathbf{Z}_{15}^{\times}$ are the congruence classes {1, 2, 4, 7, 8, 11, 13, 14}; there are $\varphi(15) = 8$ of them.

```
x     x, x^2, x^3, ... (mod 15)
1 :   1
2 :   2,  4,  8, 1
4 :   4,  1
7 :   7,  4, 13, 1
8 :   8,  4,  2, 1
11 :  11,  1
13 :  13,  4,  7, 1
14 :  14,  1
```

Since there is no number whose order is 8, there are no primitive roots modulo 15. Indeed, $\lambda(15) = 4$, where λ is the Carmichael function. (sequence A002322 in the OEIS)

Table of primitive roots

Numbers which have a primitive root are

> 1, 2, 3, 4, 5, 6, 7, 9, 10, 11, 13, 14, 17, 18, 19, 22, 23, 25, 26, 27, 29, 31, 34, 37, 38, 41, 43, 46, 47, 49, 50, 53, 54, 58, 59, 61, 62, 67, 71, 73, 74, 79, 81, 82, 83, 86, 89, 94, 97, 98, 101, 103, 106, 107, 109, 113, 118, 121, 122, 125, 127, 131, 134, 137, 139, 142, 146, 149, ... (sequence A033948 in the OEIS)

This is Gauss's table of the primitive roots from the *Disquisitiones*. Unlike most modern authors he did not always choose the smallest primitive root. Instead, he chose 10 if it is a primitive root; if it isn't, he chose whichever root gives 10 the smallest index, and, if there is more than one, chose the smallest of them. This is not only to make hand calculation easier, but is used in § VI where the periodic decimal expansions of rational numbers are investigated.

The rows of the table are labelled with the prime powers (excepting 2, 4, and 8) less than 100; the second column is a primitive root modulo that number. The columns are labelled with the primes less than 100. The entry in row p, column q is the index of q modulo p for the given root.

> For example, in row 11, 2 is given as the primitive root, and in column 5 the entry is 4. This means that $2^4 = 16 \equiv 5 \pmod{11}$.

For the index of a composite number, add the indices of its prime factors.

> For example, in row 11, the index of 6 is the sum of the indices for 2 and 3: $2^{1+8} = 512 \equiv 6 \pmod{11}$. The index of 25 is twice the index 5: $2^8 = 256 \equiv 25 \pmod{11}$. (Of course, since $25 \equiv 3 \pmod{11}$, the entry for 3 is 8).

The table is straight forward for the odd prime powers. But the powers of 2 (16, 32, and 64) do not have primitive roots; instead, the powers of 5 account for one-half of the odd numbers less than the power of 2, and their negatives modulo the power of 2 account for the other half. All powers of 5 are ≡ 5 or 1 (mod 8); the columns headed by numbers ≡ 3 or 7 (mod 8) contain the index of its negative. (Sequence A185189 and A185268 in OEIS)

> For example, modulo 32 the index for 7 is 2, and $5^2 = 25 \equiv -7 \pmod{32}$, but the entry for 17 is 4, and $5^4 = 625 \equiv 17 \pmod{32}$.

Primitive roots and indices
(other columns are the indices of integers under respective column headings)

n	root	2	3	5	7	11	13	17	19	23	29	31	37	41	43	47	53	59	61	67	71	73	79	83	89	97
3	**2**	1																								
5	**2**	1	3																							
7	**3**	2	1	5																						
9	**2**	1	*	5	4																					
11	**2**	1	8	4	7																					
13	**6**	5	8	9	7	11																				
16	**5**	*	3	1	2	1	3																			
17	**10**	10	11	7	9	13	12																			
19	**10**	17	5	2	12	6	13	8																		
23	**10**	8	20	15	21	3	12	17	5																	
25	**2**	1	7	*	5	16	19	13	18	11																
27	**2**	1	*	5	16	13	8	15	12	11																
29	**10**	11	27	18	20	23	2	7	15	24																
31	**17**	12	13	20	4	29	23	1	22	21	27															
32	**5**	*	3	1	2	5	7	4	7	6	3	0														
37	**5**	11	34	1	28	6	13	5	25	21	15	27														
41	**6**	26	15	22	39	3	31	33	9	36	7	28	32													
43	**28**	39	17	5	7	6	40	16	29	20	25	32	35	18												
47	**10**	30	18	17	38	27	3	42	29	39	43	5	24	25	37											
49	**10**	2	13	41	*	16	9	31	35	32	24	7	38	27	36	23										
53	**26**	25	9	31	38	46	28	42	41	39	6	45	22	33	30	8										
59	**10**	25	32	34	44	45	28	14	22	27	4	7	41	2	13	53	28									
61	**10**	47	42	14	23	45	20	49	22	39	25	13	33	18	41	40	51	17								
64	**5**	*	3	1	10	5	15	12	7	14	11	8	9	14	13	12	5	1	3							
67	**12**	29	9	39	7	61	23	8	26	20	22	43	44	19	63	64	3	54	5							
71	**62**	58	18	14	33	43	27	7	38	5	4	13	30	55	44	17	59	29	37	11						
73	**5**	8	6	1	33	55	59	21	62	46	35	11	64	4	51	31	53	5	58	50	44					
79	**29**	50	71	34	19	70	74	9	10	52	1	76	23	21	47	55	7	17	75	54	33	4				
81	**11**	25	*	35	22	1	38	15	12	5	7	14	24	29	10	13	45	53	4	20	33	48	52			
83	**50**	3	52	81	24	72	67	4	59	16	36	32	60	38	49	69	13	20	34	53	17	43	47			
89	**30**	72	87	18	7	4	65	82	53	31	29	57	77	67	59	34	10	45	19	32	26	68	46	27		
97	**10**	86	2	11	53	82	83	19	27	79	47	26	41	71	44	60	14	65	32	51	25	20	42	91	18	
n	root	**2**	**3**	**5**	**7**	**11**	**13**	**17**	**19**	**23**	**29**	**31**	**37**	**41**	**43**	**47**	**53**	**59**	**61**	**67**	**71**	**73**	**79**	**83**	**89**	**97**

The following table lists the primitive roots modulo n for $n \leq 72$:

n	primitive roots modulo n	order (A000010)	n	primitive roots modulo n	order (A000010)
1	0	1	37	2, 5, 13, 15, 17, 18, 19, 20, 22, 24, 32, 35	36
2	1	1	38	3, 13, 15, 21, 29, 33	18
3	2	2	39		24
4	3	2	40		16
5	2, 3	4	41	6, 7, 11, 12, 13, 15, 17, 19, 22, 24, 26, 28, 29, 30, 34, 35	40
6	5	2	42		12
7	3, 5	6	43	3, 5, 12, 18, 19, 20, 26, 28, 29, 30, 33, 34	42
8		4	44		20
9	2, 5	6	45		24
10	3, 7	4	46	5, 7, 11, 15, 17, 19, 21, 33, 37, 43	22
11	2, 6, 7, 8	10	47	5, 10, 11, 13, 15, 19, 20, 22, 23, 26, 29, 30, 31, 33, 35, 38, 39, 40, 41, 43, 44, 45	46
12		4	48		16
13	2, 6, 7, 11	12	49	3, 5, 10, 12, 17, 24, 26, 33, 38, 40, 45, 47	42
14	3, 5	6	50	3, 13, 17, 23, 27, 33, 37, 47	20
15		8	51		32
16		8	52		24
17	3, 5, 6, 7, 10, 11, 12, 14	16	53	2, 3, 5, 8, 12, 14, 18, 19, 20, 21, 22, 26, 27, 31, 32, 33, 34, 35, 39, 41, 45, 48, 50, 51	52
18	5, 11	6	54	5, 11, 23, 29, 41, 47	18
19	2, 3, 10, 13, 14, 15	18	55		40
20		8	56		24
21		12	57		36
22	7, 13, 17, 19	10	58	3, 11, 15, 19, 21, 27, 31, 37, 39, 43, 47, 55	28
23	5, 7, 10, 11, 14, 15, 17, 19, 20, 21	22	59	2, 6, 8, 10, 11, 13, 14, 18, 23, 24, 30, 31, 32, 33, 34, 37, 38, 39, 40, 42, 43, 44, 47, 50, 52, 54, 55, 56	58
24		8	60		16
25	2, 3, 8, 12, 13, 17, 22, 23	20	61	2, 6, 7, 10, 17, 18, 26, 30, 31, 35, 43, 44, 51, 54, 55, 59	60
26	7, 11, 15, 19	12	62	3, 11, 13, 17, 21, 43, 53, 55	30
27	2, 5, 11, 14, 20, 23	18	63		36
28		12	64		32
29	2, 3, 8, 10, 11, 14, 15, 18, 19, 21, 26, 27	28	65		48
30		8	66		20
31	3, 11, 12, 13, 17, 21, 22, 24	30	67	2, 7, 11, 12, 13, 18, 20, 28, 31, 32, 34, 41, 44, 46, 48, 50, 51, 57, 61, 63	66
32		16	68		32
33		20	69		44
34	3, 5, 7, 11, 23, 27, 29, 31	16	70		24
35		24	71	7, 11, 13, 21, 22, 28, 31, 33, 35, 42, 44, 47, 52, 53, 55, 56, 59, 61, 62, 63, 65, 67, 68, 69	70
36		12	72		24

It is conjectured that every natural number except perfect squares appears in the list infinitely.

The sequence of smallest primitive roots mod n (which is not the same as the sequence of primitive roots in Gauss's table) are

> 0, 1, 2, 3, 2, 5, 3, 0, 2, 3, 2, 0, 2, 3, 0, 0, 3, 5, 2, 0, 0, 7, 5, 0, 2, 7, 2, 0, 2, 0, 3, 0, 0, 3, 0, 0, 2, 3, 0, 0, 6, 0, 3, 0, 0, 5, 5, 0, 3, 3, 0, 0, 2, 5, 0, 0, 0, 3, 2, 0, 2, 3, 0, 0, 0, 0, 2, 0, 0, 0, 7, 0, 5, 5, 0, ... (sequence A046145 in the OEIS)

For prime n, they are

> 1, 2, 2, 3, 2, 2, 3, 2, 5, 2, 3, 2, 6, 3, 5, 2, 2, 2, 2, 7, 5, 3, 2, 3, 5, 2, 5, 2, 6, 3, 3, 2, 3, 2, 2, 6, 5, 2, 5, 2, 2, 2, 19, 5, 2, 3, 2, 3, 2, 6, 3, 7, 7, 6, 3, 5, 2, 6, 5, 3, 3, 2, 5, 17, 10, 2, 3, 10, 2, 2, 3, 7, 6, 2, 2, ... (sequence A001918 in the OEIS)

The largest primitive roots modulo n are

> 0, 1, 2, 3, 3, 5, 5, 0, 5, 7, 8, 0, 11, 5, 0, 0, 14, 11, 15, 0, 0, 19, 21, 0, 23, 19, 23, 0, 27, 0, 24, 0, 0, 31, 0, 0, 35, 33, 0, 0, 35, 0, 34, 0, 0, 43, 45, 0, 47, 47, 0, 0, 51, 47, 0, 0, 0, 55, 56, 0, 59, 55, 0, 0, 0, 0, 63, 0, 0, 0, 69, 0, 68, 69, 0, ... (sequence A046146 in the OEIS)

For prime n, they are

1, 2, 3, 5, 8, 11, 14, 15, 21, 27, 24, 35, 35, 34, 45, 51, 56, 59, 63, 69, 68, 77, 80, 86, 92, 99, 101, 104, 103, 110, 118, 128, 134, 135, 147, 146, 152, 159, 165, 171, 176, 179, 189, 188, 195, 197, 207, 214, 224, 223, ... (sequence A071894 in the OEIS)

Number of primitive roots mod n are

1, 1, 1, 1, 2, 1, 2, 0, 2, 2, 4, 0, 4, 2, 0, 0, 8, 2, 6, 0, 0, 4, 10, 0, 8, 4, 6, 0, 12, 0, 8, 0, 0, 8, 0, 0, 12, 6, 0, 0, 16, 0, 12, 0, 0, 10, 22, 0, 12, 8, 0, 0, 24, 6, 0, 0, 0, 12, 28, 0, 16, 8, 0, 0, 0, 0, 20, 0, 0, 0, 24, 0, 24, 12, 0, ... (sequence A046144 in the OEIS)

For prime n, they are

1, 1, 2, 2, 4, 4, 8, 6, 10, 12, 8, 12, 16, 12, 22, 24, 28, 16, 20, 24, 24, 24, 40, 40, 32, 40, 32, 52, 36, 48, 36, 48, 64, 44, 72, 40, 48, 54, 82, 84, 88, 48, 72, 64, 84, 60, 48, 72, 112, 72, 112, 96, 64, 100, 128, 130, 132, 72, 88, 96, ... (sequence A008330 in the OEIS)

Smallest prime > n with primitive root n are

2, 3, 5, 0, 7, 11, 11, 11, 0, 17, 13, 17, 19, 17, 19, 0, 23, 29, 23, 23, 23, 31, 47, 31, 0, 29, 29, 41, 41, 41, 47, 37, 43, 41, 37, 0, 59, 47, 47, 47, 47, 59, 47, 47, 47, 67, 59, 53, 0, 53, ... (sequence A023049 in the OEIS)

Smallest prime (not necessarily exceeding n) with primitive root n are

2, 3, 2, 0, 2, 11, 2, 3, 2, 7, 2, 5, 2, 3, 2, 0, 2, 5, 2, 3, 2, 5, 2, 7, 2, 3, 2, 5, 2, 11, 2, 3, 2, 19, 2, 0, 2, 3, 2, 7, 2, 5, 2, 3, 2, 11, 2, 5, 2, 3, 2, 5, 2, 7, 2, 3, 2, 5, 2, 19, 2, 3, 2, 0, 2, 7, 2, 3, 2, 19, 2, 5, 2, 3, 2, ... (sequence A056619 in the OEIS)

Arithmetic facts

Gauss proved[6] that for any prime number p (with the sole exception of $p = 3$), the product of its primitive roots is congruent to 1 modulo p.

He also proved[7] that for any prime number p, the sum of its primitive roots is congruent to $\mu(p-1)$ modulo p, where μ is the Möbius function.

> For example,
>
> $p = 3$, $\mu(2) = -1$. The primitive root is 2.
> $p = 5$, $\mu(4) = 0$. The primitive roots are 2 and 3.
> $p = 7$, $\mu(6) = 1$. The primitive roots are 3 and 5.
> $p = 31$, $\mu(30) = -1$. The primitive roots are 3, 11, 12, 13, 17 ≡ −14, 21 ≡ −10, 22 ≡ −9, and 24 ≡ −7.
>
> Their product 970377408 ≡ 1 (mod 31) and their sum 123 ≡ −1 (mod 31).
>
> 3 × 11 = 33 ≡ 2
> 12 × 13 = 156 ≡ 1
> (−14) × (−10) = 140 ≡ 16
> (−9) × (−7) = 63 ≡ 1, and 2 × 1 × 16 × 1 = 32 ≡ 1 (mod 31).

Finding primitive roots

No simple general formula to compute primitive roots modulo n is known.[8][9] There are however methods to locate a primitive root that are faster than simply trying out all candidates. If the multiplicative order of a number m modulo n is equal to $\varphi(n)$ (the order of $\mathbf{Z}_n^\times$), then it is a primitive root. In fact the converse is true: If m is a primitive root modulo n, then the multiplicative order of m is $\varphi(n)$. We can use this to test for primitive roots.

First, compute $\varphi(n)$. Then determine the different prime factors of $\varphi(n)$, say p_1, ..., p_k. Now, for every element m of $\mathbf{Z}_n^*$, compute

$$m^{\varphi(n)/p_i} \mod n \qquad \text{for } i = 1, \ldots, k$$

using a fast algorithm for modular exponentiation such as exponentiation by squaring. A number m for which these k results are all different from 1 is a primitive root.

The number of primitive roots modulo n, if there are any, is equal to[10]

$$\varphi(\varphi(n))$$

since, in general, a cyclic group with r elements has $\varphi(r)$ generators. For prime n, this equals $\varphi(n-1)$, and since $n/\varphi(n-1) = O(\log\log n)$ the generators are very common among {2,...,n-1} and thus it is relatively easy to find one.[11]

If g is a primitive root modulo p, then g is a primitive root modulo all powers p^k unless $g^{p-1} \equiv 1 \pmod{p^2}$; in that case, $g + p$ is.[12]

If g is a primitive root modulo p^k, then g or $g + p^k$ (whichever one is odd) is a primitive root modulo $2p^k$.[12]

Finding primitive roots modulo p is also equivalent to finding the roots of the $(p-1)^{th}$ cyclotomic polynomial modulo p.

Order of magnitude of primitive roots

The least primitive root g_p modulo p (in the range 1, 2, ..., $p - 1$) is generally small.

Upper bounds

Burgess (1962) proved[13] that for every ε > 0 there is a C such that $g_p \leq Cp^{\frac{1}{4}+\epsilon}$.

Grosswald (1981) proved[13] that if $p > e^{e^{24}}$, then $g_p < p^{0.499}$.

Shoup (1990, 1992) proved,[14] assuming the generalized Riemann hypothesis, that $g_p = O(\log^6 p)$.

Lower bounds

Fridlander (1949) and Salié (1950) proved[13] that there is a positive constant C such that for infinitely many primes $g_p > C \log p$.

It can be proved[13] in an elementary manner that for any positive integer M there are infinitely many primes such that $M < g_p < p - M$.

Applications

A primitive root modulo n is often used in cryptography, including the Diffie–Hellman key exchange scheme.

See also

- Artin's conjecture on primitive roots
- Dirichlet character
- Full reptend prime
- Gauss's generalization of Wilson's theorem
- Multiplicative order
- Quadratic residue
- Root of unity modulo n

Notes

1. http://www.brynmawr.edu/math/people/stromquist/numbers/primitive.html
2. Weisstein, Eric W. "Modulo Multiplication Group" (http://mathworld.wolfram.com/ModuloMultiplicationGroup.html). *MathWorld*.
3. Primitive root (http://www.encyclopediaofmath.org/index.php/Primitive_root), Encyclopedia of Mathematics.
4. Vinogradov 2003, pp. 105–121, § VI PRIMITIVE ROOTS AND INDICES.
5. Vinogradov 2003, p. 106.
6. Gauss & Clarke 1986, arts. 80.
7. Gauss & Clarke 1986, arts. 81.
8. von zur Gathen & Shparlinski 1998, pp. 15–24: "One of the most important unsolved problems in the theory of finite fields is designing a fast algorithm to construct primitive roots."
9. Robbins 2006, p. 159: "There is no convenient formula for computing [the least primitive root]."
10. (sequence A010554 in the OEIS)
11. Donald E. Knuth, *The Art of Computer Programming, vol. 2: Seminumerical Algorithms*, 3rd edition, section 4.5.4, p. 391 (Addison–Wesley, 1998).
12. Cohen 1993, p. 26.
13. Ribenboim 1996, p. 24.
14. Bach & Shallit 1996, p. 254.

References

The *Disquisitiones Arithmeticae* has been translated from Gauss's Ciceronian Latin into English and German. The German edition includes all of his papers on number theory: all the proofs of quadratic reciprocity, the determination of the sign of the Gauss sum, the investigations into biquadratic reciprocity, and unpublished notes.

- Bach, Eric; Shallit, Jeffrey (1996), *Algorithmic Number Theory (Vol I: Efficient Algorithms)*, Cambridge: The MIT Press, ISBN 0-262-02405-5.
- Cohen, Henri (1993), *A Course in Computational Algebraic Number Theory*, Berlin: Springer, ISBN 3-540-55640-0.
- Gauss, Carl Friedrich; Clarke, Arthur A. (translator) (1986), *Disquisitiones Arithmeticae* (2nd, corrected ed.), New York: Springer, ISBN 0-387-96254-9 [in English].
- Gauss, Carl Friedrich; Maser, H. (translator) (1965), *Untersuchungen über höhere Arithmetik [Studies on higher arithmetic]* (2nd ed.), New York: Chelsea, ISBN 0-8284-0191-8 [in German].
- Ribenboim, Paulo (1996), *The New Book of Prime Number Records*, New York: Springer, ISBN 0-387-94457-5.
- Robbins, Neville (2006), *Beginning Number Theory* (https://books.google.com/books?id=TtLMrKDsDuIC&pg=PA159), Jones & Bartlett Learning, ISBN 978-0-7637-3768-9.
- Vinogradov, I. M. (2003), "§ VI PRIMITIVE ROOTS AND INDICES", *Elements of Number Theory* (https://books.google.co.jp/books?id=xIIfdGPM9t4C&lpg=PR3&hl=ja&pg=PA105#v=onepage&q&f=false), Mineola, NY: Dover Publications, pp. 105–121, ISBN 978-0-486-49530-9.
- von zur Gathen, Joachim; Shparlinski, Igor (1998), "Orders of Gauss periods in finite fields", *Applicable Algebra in Engineering, Communication and Computing*, **9** (1), doi:10.1007/s002000050093 (https://doi.org/10.1007/s002000050093), MR 1624824 (https://www.ams.org/mathscinet-getitem?mr=1624824).

Further reading

- Ore, Oystein (1988), *Number Theory and Its History*, Dover, pp. 284–302, ISBN 0-486-65620-9.

External links

- Weisstein, Eric W. "Primitive Root" (http://mathworld.wolfram.com/PrimitiveRoot.html). *MathWorld*.
- "Quadratic Residues and Primitive Roots" (http://www.math.mtu.edu/mathlab/COURSES/holt/dnt/quadratic4.html). Michigan Tech.
- "Primitive Roots Calculator" (http://www.bluetulip.org/programs/primitive.html). BlueTulip.