Zeitschrift: Elemente der Mathematik

Herausgeber: Schweizerische Mathematische Gesellschaft

Band: 37 (1982)

Heft: 4

Artikel: On primitive roots

Autor: Ecker, A.

DOI: https://doi.org/10.5169/seals-36395

6 C.G.J. Jacobi: Geometrische Theoreme. J. reine angew. Math. *12* (1834) oder *73*, 179-206 (1871), oder: Gesammelte Werke, Bd. 7, S. 42-68. Verlag G. Reimer, Berlin 1891.
7 K. Killian und P. Meissl: Einige Grundaufgaben der räumlichen Trilateration und ihre gefährlichen Örter. Dt. Geod. Komm. Bayer. Akad. Wiss. (A) *61*, 65-72 (1969).
8 H. Stachel: Eine Anwendung der kinematischen Abbildung. In Vorbereitung.
9 H. Stachel: Bemerkungen zur räumlichen Trilateration. In Vorbereitung.
10 W. Wunderlich: Gefährliche Annahmen der Trilateration und bewegliche Fachwerke I. Z. angew. Math. Mech. *57*, 297-304 (1977).

 0013-6018/82/040097-07$1.50 ± 0.20/0

On primitive roots

Baum [2] has given useful criteria for certain primitive roots. Wilansky [6] pointed out that these results can be obtained without use of quadratic reciprocity. The purpose of this note is to derive their theorems and to obtain some more results with a quite simple counting method. We shall deal with odd primes p. We assume standard results on quadratic residues and primitive roots. An integer a relatively prime to p belongs to the exponent $k>0$, modulo p, if $a^k \equiv 1 \pmod{p}$ and $a^n \not\equiv 1 \pmod{p}$ for $0<n<k$. A primitive root modulo p is a residue which belongs to the exponent $p-1$. There are $\varphi(p-1)$ primitive roots modulo p, where $\varphi(x)$ is the Euler phi-function or totient. Euler's totient has the following property: if m is odd then $\varphi(2^n \cdot m)=2^{n-1}\varphi(m)\,(n \geq 1)$ and $\varphi(2^n \cdot m)=2^n \varphi(m)$ if m is even. A quadratic residue, modulo p, is an integer $a \neq 0$ such that $x^2 \equiv a \pmod{p}$ has solutions. QR (QNR) denotes the set of residues, modulo p, which are quadratic residues (non-residues). With respect to the property of being a primitive root, modulo p, these sets are denoted by PR(NPR). We note the following familiar results: a is a quadratic residue modulo p if and only if $a^{(p-1)/2} \equiv 1 \pmod{p}$. This result is known as Euler's criterion. From Euler's criterion it follows that $(-1/p)=(-1)^{(p-1)/2}$, where (a/p) is the Legendre symbol, defined by $(a/p)=+1$ if $a \in \mathrm{QR}$, $(a/p)=-1$ if $a \in \mathrm{QNR}$. Gauss has given a theorem - known as Gauss' lemma - that puts the information contained in Euler's criterion into a slightly different form. Gauss' lemma makes it possible to evaluate $(2/p)$, $(3/p)$, $(7/p)$.
The Legendre symbol has the properties:

$$\left(\frac{a}{p}\right)\cdot\left(\frac{b}{p}\right)=\left(\frac{a\cdot b}{p}\right), \qquad \left(\frac{a}{p}\right)=\left(\frac{b}{p}\right) \quad \text{if} \quad a \equiv b \pmod{p}$$

where a, b are relatively prime to p. This makes it possible to calculate $(-a/p)$ if (a/p) is known. We give a list of values (a/p) needed in the sequel.

$$\left(\frac{-1}{p}\right)=\begin{cases}+1 & \text{if} \quad p \equiv 1 \pmod{4}\\ -1 & \text{if} \quad p \equiv -1 \pmod{4}\end{cases}$$

$$\left(\frac{2}{p}\right)=\begin{cases}+1 & \text{if } p\equiv \pm 1 \pmod 8\\ -1 & \text{if } p\equiv \pm 3 \pmod 8\end{cases}$$

$$\left(\frac{3}{p}\right)=\begin{cases}+1 & \text{if } p\equiv \pm 1 \pmod{12}\\ -1 & \text{if } p\equiv \pm 5 \pmod{12}\end{cases}$$

$$\left(\frac{-7}{p}\right)=\begin{cases}+1 & \text{if } p\equiv 1,2,4 \pmod 7\\ -1 & \text{if } p\equiv 3,5,6 \pmod 7\end{cases}$$

$$\left(\frac{-2}{p}\right)=\begin{cases}+1 & \text{if } p\equiv 1,3 \pmod 8\\ -1 & \text{if } p\equiv -1,-3 \pmod 8\end{cases}$$

$$\left(\frac{-3}{p}\right)=\begin{cases}+1 & \text{if } p\equiv 1 \pmod 6\\ -1 & \text{if } p\equiv -1 \pmod 6\end{cases}$$

Clearly no number is simultaneously a quadratic residue and a primitive root modulo p; and there are exactly $(p-1)/2$ quadratic residues modulo p. This means $\mathrm{PR}\subset\mathrm{QNR}$ and $|\mathrm{QR}|=(p-1)/2$, where $|M|$ denotes the number of elements in a finite set M.

Lemma 1. *$|QNR|=|PR|+|NPR\cap QNR|$ or with $D=|NPR\cap QNR|=|QNR\backslash PR|$*

$$\frac{p-1}{2}=\varphi(p-1)+D, \qquad D\geq 0. \tag{1}$$

The proof of lemma 1 is quite clear from what we said above.

Lemma 2. *If $p\equiv 1 \pmod 4$, $p=4q+1$ $(q\geq 1)$, then D is even and $4\mid D$ if q is even, $2\parallel D$ if q is odd and $q>1$. D is odd if $p\equiv -1 \pmod 4$, $p=2q+1$ $(q\geq 1$, q odd$)$ except for $q=1, p=3$ where $D=0$.*

Proof: $D=(p-1)/2-\varphi(p-1)$.
$p=4q+1$: $D=2q-\varphi(4q)$ and $2\mid\varphi(4q)$ proves that D is even; q even means $\varphi(4q)=4\varphi(q)$, $4\mid 2q$ and $4\mid D$ follows, q odd gives $\varphi(4q)=2\varphi(q)$, $D=2(q-\varphi(q))$ and $2\nmid(q-\varphi(q))$ except for $q=1$, but then $p=5$ and $D=0$. $p=2q+1$, q odd: $D=q-\varphi(q)$ and D is odd except for $q=1$.
Naturally we now ask whether there is - excepting 3 and 5 - any possibility that $D=0$ happens, that means that all quadratic nonresidues are primitive roots. If

$-1 \in \mathrm{QNR}$ or $(-1/p) = -1$ $D=0$ is impossible, except for $p=3$, because $(-1)^2 \equiv 1 \pmod p$ and the exponent of -1 modulo p is 2, $-1 \in \mathrm{QNR} \setminus \mathrm{PR}$ except in case $p-1=2$, that is $p=3$. If $p \equiv -1 \pmod 4$ then $(-1/p) = -1$, hence $D \geq 1$ if $p > 3$ and $p \equiv -1 \pmod 4$.

Theorem 1. *$D=0$ if and only if $p = 2^{2^n}+1 = F(n)$ $(n \geq 0)$, the n-th Fermat number.*

Proof: If $D=0$, then $p=3=F(0)$ or $p=4q+1$ $(q \geq 1)$ and from lemma 1 one gets $(p-1)/2 = \varphi(p-1)$. This given $2q = \varphi(4q)$, q odd: $q = \varphi(q)$ implies $q=1$. q even: $q = 2\varphi(q)$, $q = 2^m \cdot r$ $(m \geq 1)$, $2 \nmid r$ this implies $r = \varphi(r)$ or $r=1$. That means $p = 2^{m+2}+1$ $(m \geq 1)$.
Thus $p = 2^t + 1$ $(t \geq 1)$, but it is well known that $t = 2^n$ $(n \geq 0)$ is necessary and these are the Fermat numbers. The converse follows by a simple computation.

Corollary 1.1. *An odd prime p is a Fermat prime if and only if all quadratic non-residues, modulo p, are primitive roots.*

Corollary 1.2. *± 3 is a primitive root modulo $p = F(n)$ $(n \geq 1)$.*

Proof: $F(n) \equiv 5 \pmod{12}$ $(n \geq 1)$ as follows from $4^m \equiv 4 \pmod{12}$. From $p \equiv 5 \pmod{12}$ we get $(\pm 3/p) = -1$ or $\pm 3 \in \mathrm{QNR}$. Corollary 1.1 completes the proof.

Corollary 1.3. *± 7 is a primitive root of $p = F(n)$ $(n \geq 2)$.*

Proof: Note that $2^4 \equiv 2 \pmod 7$ and $F(n) \equiv 3,5 \pmod 7$ $(n \geq 2)$. Thus $(-7/p) = -1$, $-7 \in \mathrm{QNR}$ and $(-1/p) = +1$ gives $(-1/p) \cdot (-7/p) = (7/p) = -1$, $7 \in \mathrm{QNR}$. Corollary 1.1 then gives the conclusion.

Theorem 2. *$D=1$ if and only if $p = 2q+1$, where q is an odd prime.*

Proof: From lemma 2 we see that $p = 2q+1$, q odd $(q > 1)$. (1) gives $q-1 = \varphi(q)$ and q necessarily is an odd prime. The converse follows by computation.

Corollary 2.1. *All quadratic nonresidues modulo p beside -1 are primitive roots if and only if $p = 2q+1$, where q is an odd prime.*

Corollary 2.2. *If p and q are odd primes, $p = 2q+1$, then $(-1)^{(q-1)/2} \cdot 2$ is a primitive root modulo p.*

Proof: If $q \equiv 1 \pmod 4$, then $2q+1 \equiv 3 \pmod 8$ but then $(2/p) = -1$, $2 \in \mathrm{QNR}$ and $2 \not\equiv -1 \pmod p$. From corollary 2.1 we see that $2 \in \mathrm{PR}$, modulo p. If $q \equiv -1 \pmod 4$ we get $2q+1 \equiv -1 \pmod 8$, i.e. $(-2/p) = -1$ or $-2 \in \mathrm{QNR}$, $-2 \not\equiv -1 \pmod p$ and $-2 \in \mathrm{PR}$.

Corollary 2.3. *If p and q are odd primes, $p = 2q+1$, then if $q \equiv 1 \pmod 4$, $q+1$ is a primitive root modulo p, while if $q \equiv -1 \pmod 4$, q is a primitive root modulo p.*

Proof: If $q \equiv 1 \pmod 4$, then from corollary 2.2 we know $(2/p) = -1$. Since $2(q+1) = 2q+2 \equiv 1 \pmod p$ we have

$$\left(\frac{2}{p}\right) \cdot \left(\frac{q+1}{p}\right) = \left(\frac{1}{p}\right) = +1 \quad \text{and thus} \quad \left(\frac{q+1}{p}\right) = -1 .$$

Hence $q+1 \in$ QNR and $q+1 \not\equiv -1 \pmod p$ means $q+1 \in$ PR. If $q \equiv -1 \pmod 4$ the proof is similar: $2q \equiv -1 \pmod p$ or $(-2) \cdot q \equiv 1 \pmod p$ implies $(-2/p) \cdot (q/p) = +1$ and this again gives $q \in$ PR.
Note that in corollary 2.3 one can write the conclusion as: $(-1)^{(q+1)/2} \cdot q$ is a primitive root modulo p.

Remark: Theorem 1 is exercise 3.8, No. 11, in Agnew [1], p. 144, while corollary 1.2 is given by Trost [5], IV.25, p. 40, and corollary 1.3 is just problem 3, chap. 5.3, in Le Veque [4], p. 69. Corollaries 2.1, 2.2 and 2.3 are what Baum [2] proved but compare with theorem 5-6 (b), (c) in [4], p. 68.

Theorem 3. *$D=2$ if and only if $p=4q+1$, where q is an odd prime, and in this case $a \in QNR \setminus PR$ iff a belongs to the exponent 4 modulo p.*

Proof: Half of the theorem is trivial, we prove the rest. If $D=2$, then $(p-1)/2 = \varphi(p-1)+2$ or $2q = \varphi(4q)+2$, because lemma 2 gives $p=4q+1$ and q is odd. Therefore $2q = 2\varphi(q)+2$ or $q-1 = \varphi(q)$ and q is an odd prime. If $a \in$ QNR\PR, then $a^k \equiv 1 \pmod p$, where $k \mid p-1$ $(k \neq p-1)$ is the exponent of a modulo p. Now $p-1 = 4q$ and $a^{2q} \equiv -1 \pmod p$ from Euler's criterion. Hence $k \nmid 2q$ while q is an odd prime, thus $k=4$.

Corollary 3.1. *± 2 is a primitive root of $p=4q+1$ if q is an odd prime.*

Proof: From $p=4q+1$, q an odd prime it follows that $p \equiv -3 \pmod 8$. Hence $(\pm 2/p) = -1$ or $\pm 2 \in$ QNR. But $2^4 \equiv 1 \pmod p$ means $p=3$ or $p=5$ while $4q+1 \geq 13$. An application of theorem 3 completes the proof.

Corollary 3.2. *$2q$, $2q+1$ are primitive roots modulo $p=4q+1$, if q is an odd prime.*

Proof: First of all note that $2q+1 \equiv -2q \pmod p$. Therefore it is enough to show that $2q$ is a primitive root modulo p. $2(2q) \equiv -1 \pmod p$ gives $(2/p) \cdot (2q/p) = (-1/p) = +1$. From corollary 3.1 we know $(2/p) = -1$, hence $(2q/p) = -1$. Next we have to prove $(2q)^4 \not\equiv 1 \pmod p$. $(2q)^4 = (4q)^2 \cdot q^2$ and $(4q)^2 \equiv 1 \pmod p$ gives $(2q)^4 \equiv q^2 \pmod p$. But $q^2 - 1 = (q+1) \cdot (q-1)$ and from $q^2 \equiv (2q)^4 \equiv 1 \pmod p$ $p \mid q+1$ or $p \mid q-1$. It is easy to see that this cannot happen. This completes the proof.

Remark: For corollary 3.1 see theorem 5-6 (a) in [4], p. 68.

Theorem 4. *$D = 2^n$ $(n \geq 2)$ if and only if $p = 2^{n+1} \cdot r + 1 = 2D \cdot r + 1$, where r is an odd prime, and in this case $a \in QNR \setminus PR$ iff a belongs to the exponent $2D$ modulo p.*

Proof: From lemma 2 we see that $p=4q+1$ and $q=2^m \cdot r\,(m \geq 1)$, r odd. Hence from (1) $2q=4\varphi(q)+2^n$ or $q-2^{n-1}=2\varphi(q)$. $q=2^m \cdot r$ gives $2^m \cdot r-2^{n-1}=2^m \cdot \varphi(r)$ hence $r \neq 1$ and $2 \mid \varphi(r)$.
If $n-1<m$ we rewrite $2^{n-1}=2^m(r-\varphi(r))$ or $1=2^{m-n+1}(r-\varphi(r))$, a contradiction. If $n-1>m$ write $2^m \cdot r=2^m(\varphi(r)+2^{n-m-1})$ where $2 \mid (\varphi(r)+2^{n-m-1})$ but $2 \nmid r$, a contradiction. Hence $m=n-1$. This gives $r-1=\varphi(r)$ and r is an odd prime. The converse is almost trivial. If $a \in$ QNR and k is the exponent of a modulo p, then $a^{D \cdot r} \equiv -1 \pmod{p}$ and $k \mid 2D \cdot r$. Thus $k \nmid D \cdot r$ and r is prime. Therefore $k=2D$ since $k \neq 2D \cdot r$ and the proof is complete.

Lemma 3. *Let $p=2D \cdot r+1$, $D=2^n\,(n \geq 2)$ as in theorem 4. Then, except possibly for $r=3$, ± 3 resp. ± 6 is a primitive root modulo p if and only if 3^{2D} resp. $6^{2D} \not\equiv 1 \pmod{p}$.*

Proof: Note that $4 \equiv 1 \pmod 3$ and hence $2^m \equiv 1 \pmod 3$ if m is even, $2^m \equiv 2 \pmod 3$ if m is odd. If $m=n+1$, then $p \equiv r+1$ or $2r+1 \pmod 3$ according as n is odd or even. $r \equiv 1,2 \pmod 3$ always gives $p \equiv 2 \pmod 3$, $p \equiv 0 \pmod 3$ is not possible. Hence $3 \mid p+1$, trivially $2 \mid p+1$, therefore $6 \mid p+1$ or $p \equiv -1 \pmod 6$.
From our list of computed Legendre symbols we see $(-3/p)=-1$. Taking into account $-1, 2 \in$ QR and theorem 4 the proof is complete.

Corollary 4.1. *If $p=8 \cdot r+1$, where r is an odd prime, then ± 6 is a primitive root modulo p. ± 3 is a primitive root modulo p if $r \neq 5$.*

Proof: From theorem 4 we see that $D=4$ and lemma 3 shows that one has to consider 3^8-1, 6^8-1 modulo p. Note that $r=3$ is not possible. The computation gives

$$3^8-1=6560=2^5 \cdot 5 \cdot 41,$$
$$6^8-1=1\,679\,615=5 \cdot 7 \cdot 37 \cdot 1297.$$

It is now easy to check that (except for $r=5$) $p=8r+1$ will never divide either 3^8-1 or 6^8-1.

Corollary 4.2. *If $p=16 \cdot r+1$, where r is an odd prime, then ± 3, ± 6 are primitive roots modulo p.*

Proof: $D=8$ and

$$3^{16}-1=43\,046\,720=2^6 \cdot 5 \cdot 17 \cdot 41 \cdot 193,$$
$$6^{16}-1=5 \cdot 7 \cdot 17 \cdot 37 \cdot 1297 \cdot 98801$$

($r=3$ again is impossible). A simple consideration as in the foregoing corollary now completes the proof.
Note that $p=2^{n+2} \cdot r+1$, r an integer, are just the prime divisors of $F(n)$.

Historical remarks: Most of the above results were known to nineteenth century mathematicians, although obtained by various quite different methods (see Dickson [3], chap. VII). M.A. Stern (J. Math. 6, 147–153, 1830) proved that, if $p=2q+1$ and q are odd primes, 2 or -2 is a primitive root of p according as $p=8n+3$ or $8n+7$ (see corollary 2.2). If $p=4q+1$ and q are primes, 2 and -2 are primitive roots of p (see corollary 3.1). F.J. Richelot (J. Math. 9, 5, 1832) proved that, if $p=2^m+1$ is a prime, every quadratic nonresidue (in particular, 3) is a primitive root of p (see corollaries 1.1, 1.2). Nearly the same results were given by P. L. Tchebychef ['Theory of congruences' (in Russian), 1849]. G. Wertheim (Acta Math. *17*, 315–320, 1893) proved that any prime $2^{4n}+1$ has the primitive root 7 (see corollary 1.3). If $p=2^n \cdot q+1$ is a prime and q is an odd prime, any quadratic nonresidue a of p is a primitive root of p if $a^{2n}-1$ is not divisible by p (see lemma 3). These and other nice results on primitive roots can be derived from theorems 1–4 as corollaries (see for example in [3], p. 192, what V. Bouniakowsky proved or loc. cit., p. 199, the result of A. Cunningham).

A. Ecker,
Hahn-Meitner-Institut für Kernforschung Berlin GmbH

REFERENCES

1 J. Agnew: Explorations in number theory. Wadsworth, Belmont 1972.
2 J.D. Baum: A note on primitive roots. Math. Mag. *38*, 12–14 (1965).
3 L.E. Dickson: History of the theory of numbers, vol. I. Chelsea, New York 1971.
4 W.J. Le Veque: Topics in number theory, vol. I. Addison-Wesley, Reading, Mass., 1956.
5 E. Trost: Primzahlen. Birkhäuser, Basel 1953.
6 A. Wilansky: Primitive roots without quadratic reciprocity. Math. Mag. *49*, 146 (1976).

 0013-6018/82/040103-06$1.50 ± 0.20/0

Kleine Mitteilungen

A homeomorphism of Q with Q as an orbit

The following result can be deduced from a theorem proved by Besicovitch [1] in which an autohomeomorphism h of the real plane is constructed such that for some $x \in \mathbf{R}^2$

$$\{h^n(n) \mid n \in \mathbf{Z}\} \quad \text{is dense in} \quad \mathbf{R}^2.$$

We give a direct proof for the consequence.

Proposition. *There exists an autohomeomorphism h of* $\mathbf{Q}$ *with*

$$\{h^n(1) \mid n \in \mathbf{Z}\} = \mathbf{Q}.$$

Proof: Let $x_1 \in [0,1] \backslash \mathbf{Q}$ with $2x_1 < 1$ and, for $n \in \mathbf{Z}$, $x_n = nx_1 - [nx_1]$, [ ] designating