PRIMES p SUCH THAT 2 IS A PRIMITIVE ROOT MODULO p

RAYMOND N. FULLER

1. Introduction

Let a and m be integers, $m > 1$, and $\gcd(a, m)$=1. We say that a is a primitive root modulo m if $(\mathbb{Z}/m\mathbb{Z})^*$ is cyclic and a is a generator of $(\mathbb{Z}/m\mathbb{Z})^*$. The Primitive Root Theorem characterizes those moduli m such that $(\mathbb{Z}/m\mathbb{Z})^*$ is cyclic. Of course, if p is a prime, then $(\mathbb{Z}/p\mathbb{Z})^*$ is cyclic, and so there always exists a primitive root modulo p. In this paper we present some elementary results about primes p such that 2 is a primitive root modulo p.

In what follows we will make use of an equivalent though more convenient definition for a primitive root modulo m. As before, let $a, m \in \mathbb{Z}$, $m > 1$, $\gcd(a, m) = 1$. Let $\text{ord}_m(a)$ (the order of a modulo m) be the smallest positive integer k such that $a^k \equiv 1 \pmod{m}$. Such an integer k always exists, since by Euler's Theorem, we know that $a^{\phi(m)} \equiv 1 \pmod{m}$, where $\phi(n)$ denotes the Euler phi-function. Then a is a primitive root modulo m if and only if $\text{ord}_m(a) = \phi(m)$. If p is prime, then $\phi(p) = p - 1$, so a is a primitive root modulo p if and only if $\text{ord}_p(a) = p - 1$. We now collect some elementary classical results to be used later. Recall that $\text{ord}_m(a) \mid \phi(m)$, so in particular $\text{ord}_p(2) \mid p - 1$ when p is prime (note that $\text{ord}_p(2) \neq 1$). These two properties of the Legendre Symbol will also be used: If p is an odd prime, then

$$\left(\frac{2}{p}\right) \equiv 2^{(p-1)/2} \pmod{p} \tag{1}$$

$$\left(\frac{2}{p}\right) = (-1)^{(p^2-1)/8} = \begin{cases} 1, & \text{if } p \equiv 1, 7 \pmod{8} \\ -1, & \text{if } p \equiv 3, 5 \pmod{8} \end{cases} \tag{2}$$

2. Elementary Results

Proposition 1. *Let p be an odd prime. If 2 is a primitive root modulo p then 2 is a quadratic nonresidue modulo p.*

Proof. Since 2 is a primitive root modulo p, $\text{ord}_p(2) = p-1$. Assume p is a quadratic residue modulo p. Then by (1), $2^{(p-1)/2} \equiv 1 \pmod{p}$. But then

$$\text{ord}_p(2) \leq \frac{p-1}{2} < p - 1 = \text{ord}_p(2),$$

a contradiction. So 2 is a quadratic nonresidue modulo p. □

Proposition 2. *Let p be an odd prime. If 2 is a primitive root modulo p, then $p \equiv 3, 5 \pmod{8}$.*

Date: 20 October 2008.

Proof. By (2), 2 is a quadratic nonresidue modulo an odd prime p if and only if $p \equiv 3, 5 \pmod 8$. This fact together with Proposition 1 gives the desired result. $\square$

The converse of Proposition 2 does not hold in general. For example, it may be verified that 2 is not a primitive root modulo 43.

A Fermat prime is defined to be a prime of the form $2^{2^n} + 1$. A Mersenne prime is defined to be a prime of the form $2^p - 1$ with p prime. Fermat primes greater than 5 are congruent to 1 (mod 8), and Mersenne primes greater than 3 are congruent to 7 (mod 8). Proposition 2 tells us that 2 is not a primitive root modulo p whenever p is a Fermat prime greater than 5 and whenever p is a Mersenne prime greater than 3.

Proposition 3. *Let p be an odd prime. If $8 \mid p - 1$ then 2 is not a primitive root modulo p.*

Proof. If $8 \mid p-1$ then $p \equiv 1 \pmod 8$, and so by Proposition 2, 2 is not a primitive root modulo p. $\square$

If p is an odd prime, then $p - 1$ is even, and $2 \mid p - 1$. Proposition 3 tells us that if 2 is a primitive root modulo p, 2 or 4 appear in the prime factorization of $p - 1$, but no higher power of 2 can appear.

Proposition 4. *If p is a prime of the form $p = 2q + 1$ for some odd prime q, then 2 is a primitive root modulo p if and only if $q \equiv 1, 5 \pmod 8$.*

Proof. If 2 is a primitive root modulo p, then by Proposition 2, $p \equiv 3, 5 \pmod 8$. We see at once that we must have $q \equiv 1, 5 \pmod 8$. Conversely, let $q \equiv 1, 5 \pmod 8$. Now $\mathrm{ord}_p(2)$ is either q or $2q$ (it cannot be 2, since $p \geq 7$). Assume $\mathrm{ord}_p(2) = q$. Then $2^q \equiv 1 \pmod p$, and so by (1), $\left(\frac{2}{p}\right) = 1$. But by (2), this means that $p \equiv 1, 7 \pmod 8$. But since $q \equiv 1, 5 \pmod 8$, we must have $p \equiv 3 \pmod 8$, a contradiction. So, $\mathrm{ord}_p(2) = 2q$, and 2 is a primitive root modulo p. $\square$

Proposition 5. *If p is a prime of the form $p = 4q + 1$ for some odd prime q, then 2 is a primitive root modulo p.*

Proof. The smallest prime of this form is $p = 13$, and it can be verified directly that 2 is a primitive root modulo 13. For every other prime of this form, $\mathrm{ord}_p(2)$ is one of q, $2q$, or $4q$. The cases $\mathrm{ord}_p(2) = q$ and $\mathrm{ord}_p(2) = 2q$ both imply that $2^{2q} \equiv 1 \pmod p$. Then by (1), $\left(\frac{2}{p}\right) = 1$, and so by (2), we must have $p \equiv 1, 7 \pmod 8$. But since p is of the given form, $p \equiv 5 \pmod 8$, a contradiction. So, $\mathrm{ord}_p(2) = 4q$, and 2 is a primitive root modulo p. $\square$

Proposition 6. *If p is a prime of the form $p = 4q^k + 1$ for some odd prime q and some positive integer k, then $\mathrm{ord}_p(2)$ is one of $\left\{4q, 4q^2, \ldots, 4q^k\right\}$.*

Proof. As before, 13 is the smallest prime of this form, and $\mathrm{ord}_{13}(2) = 12$, so the statement holds. For all other primes of this form, $\mathrm{ord}_p(2)$ is one of

$$\{2q, 4q, 2q^2, 4q^2, \ldots, 2q^k, 4q^k\}.$$

Assume $\mathrm{ord}_p(2) = 2q^\ell$ for some $1 \leq \ell \leq k$. Then $2^{2q^\ell} \equiv 1 \pmod p$. Therefore, $2^{2q^k} \equiv 1 \pmod p$, and so $\left(\frac{2}{p}\right) = 1$ by (1). By (2), $p \equiv 1, 7 \pmod 8$. But since

p is of the given form, $p \equiv 5 \pmod 8$, a contradiction. So, $\mathrm{ord}_p(2) \neq 2q^\ell$ for any $1 \leq \ell \leq k$, and therefore $\mathrm{ord}_p(2)$ is one of $\{4q, 4q^2, \ldots, 4q^k\}$. □

Dept. of Mathematics, Statistics, and Computer Science, The University of Illinois at Chicago, 850 S. Morgan St. Chicago, IL 60607-7045

Email address: rfuller@math.uic.edu

URL: http://www.math.uic.edu/∼rfuller/