PRIMITIVE ROOTS AND 6-GERMAIN PRIMES

ABSTRACT. We consider the 6-Germain primes, namely those primes p such that $6p+1$ is also prime. By relying on a theorem of Lehmer on cubic residuacity, we express in terms of congruences the property that p is a primitive root modulo $6p+1$.

1. INTRODUCTION

If p is a prime number, a *primitive root* modulo p is an integer a coprime to p such that $(a \bmod p)$ generates, multiplicatively, the group of non-zero residues modulo p. If n is an even positive integer, we call a prime number p an *n-Germain* prime if $q := np+1$ is also a prime number.

The following results involve primitive roots and n-Germain primes:

(1) If p is an odd 2-Germain prime: every quadratic non-residue modulo q is a generator of $(\mathbb{Z}/q\mathbb{Z})^{\times}$, with the exception of $(-1 \bmod q)$. In particular, by quadratic reciprocity, p (respectively, $p+1$ as $p+1 \equiv -p \bmod q$) is a primitive root modulo q if $p \equiv 3 \bmod 4$ (respectively, $p \equiv 1 \bmod 4$). See [1, Corollaries 2.1 and 2.3]. On the other hand, if p is prime and it is a primitive root modulo $2p+1$, then p is a 2-Germain prime, see [4].

(2) If p is an odd 4-Germain prime: ± 2 are a primitive roots modulo q, see [1, Corollary 3.1].

(3) If p is an odd 6-Germain prime: 3, 5, and 7 are a primitive roots modulo q, see [2].

(4) If p is an odd 8-Germain prime: ± 6 is a primitive root modulo q; ± 3 is a primitive root modulo q if $p \neq 5$. See [1, Corollary 4.1].

(5) If p is an odd 16-Germain prime: ± 3 and ± 16 are primitive roots modulo q, see [1, Corollary 4.2].

More results can be found for example in [5, 6]. We focus on 6-Germain primes and prove the following two results:

Theorem 1. *If a prime number p is a primitive root modulo $6p+1$, then p is a 6-Germain prime.*

As a consequence of a result by Fermat, if p is a 6-Germain prime, there exist unique positive integers L and M (see Section 2) such that

$$p = \frac{1}{24}(L^2 + 27M^2 - 4)\,.$$

Theorem 2. *Let p be a 6-Germain prime, with $p \neq 2, 7$. With the above notation, p is a primitive root modulo q if and only if the following holds: $p \equiv 3 \bmod 4$; we don't have*

$$L \equiv \pm \frac{27r(r^2-1)}{9r^2-1} M \bmod p\,, \tag{1}$$

where r is an integer such that r^2 is not congruent to $\frac{1}{9}$ modulo p.

The proof of our former theorem is rather elementary, and it mimics the proof of the analogue statement for 2-Germain primes. The proof of the latter theorem consists in reformulating the condition for being a primitive root considering the structure of the group $(\mathbb{Z}/(6p+1)\mathbb{Z})^\times$, and applying a result by Lehmer on cubic residuacity.

We have tested both results with a C program for primes p up to 10^6.

2. 6-Germain primes

We begin by proving our first result:

Proof of Theorem 1. Since 2 is a 2-Germain prime, we may suppose that p is odd. Since $(\mathbb{Z}/(6p+1)\mathbb{Z})^\times$ is cyclic and $6p+1$ is odd, we have $6p+1=m^k$ for some odd prime m. If $k>1$, then we have

$$6p = m^k - 1 = (m-1)(1+m+\cdots+m^{k-1})\,.$$

As $m-1$ is even, we have $m-1 \in \{2,6,2p,6p\}$.
If $2=m-1$, then $3p = 1+3+\cdots+3^{k-1}$, which is impossible modulo 3.
If $6 = m-1$, then $p \equiv 1+m+\cdots \equiv 1 \bmod m$ so p is a square modulo m, contradicting that it is a primitive root modulo m^k.
If $m-1$ equals $2p$ or $6p$, then $1+m+\cdots+m^{k-1} \geq 1+m$ should be 3 or 1, which is impossible. □

Example 3. *The integer* 2 *(respectively,* 3*) is a* 6*-Germain prime and it is a primitive root modulo* 13 *(respectively,* 19*). The integer* 5 *is a* 6*-Germain prime but it is not a primitive root modulo* 31.

We may now suppose that p is a 6-Germain prime that is larger than 7. In particular, as p is coprime to 6, the group $(\mathbb{Z}/(6p+1)\mathbb{Z})^\times$ is isomorphic to the product of a cyclic group of oder 2, a cyclic group of order 3, and a cyclic group of order p. We deduce the following:

Remark 4. *Consider a* 6*-Germain prime $p \neq 2,3$ and set $q := 6p+1$. Then an integer a is a primitive root modulo q if and only if all of the following conditions hold:*

(i) *a is not a square modulo q*
(ii) *a is not a cube modulo q*
(iii) *$(a \bmod q)$ does not have multiplicative order* 6.

Proposition 5. *A* 6*-Germain prime $p>7$ (setting $q := 6p+1$) is a primitive root modulo q if and only if $p \equiv 3 \bmod 4$ and p is not a cube modulo q.*

Proof. We first prove that $(p \bmod q)$ does not have multiplicative order 6. Indeed, consider the decomposition

$$p^6-1=(p^2-1)(p^2+p+1)(p^2-p-1)\,.$$

If the the order of $(p \bmod q)$ would be 6, then q divides p^6-1 but not p^2-1. We deduce that q divides (p^2+p+1) or (p^2-p-1). We have a contradiction because we have

$$p^2+p+1 \equiv p(p-5) \bmod q \quad \text{and} \quad p^2-p-1 \equiv p(p+5) \bmod q$$

but q divides neither p nor $p \pm 5$. By Remark 4 we may conclude by showing that p is not a square modulo q if and only if $p \equiv 3 \bmod 4$ (which implies $q \equiv 3 \bmod 4$). Indeed, this follows from quadratic reciprocity, remarking that $(q \bmod p) = (1 \bmod p)$ is a square. □

The problem of determining whether a 6-Germain prime p is a primitive root modulo $q = 6p + 1$ is then reduced to assessing a special case of cubic reciprocity (considering that $(q \bmod p) = (1 \bmod p)$ is a cube).

2.1. **Cubic reciprocity for 6-Germain primes.** This section relies on [7]. We consider a 6-Sophie Germain prime $p > 7$, setting $q = 6p + 1$. Since $q \equiv 1 \bmod 3$ is prime,

$$q = \frac{1}{4}(L^2 + 27M^2)$$

holds for some uniquely determined positive integers L, M. Thus we can write

$$p = \frac{1}{24}(L^2 + 27M^2 - 4)\,.$$

Remark 6. *With the above notation, by Lehmer's theorem* [3] *the following holds: p is a cube modulo q if and only if $p \mid LM$ or (for at least one of the two sign choices) $L \equiv \pm\frac{9r}{2u+1}M \bmod p$, where $u \not\equiv 0, 1, -\frac{1}{2}, -\frac{1}{3} \bmod p$ and $3u+1 \equiv r^2(3u-3) \bmod p$.*

The condition $p \mid LM$ only holds for $p = 23$. The condition $p \mid LM$ is equivalent to $p \mid L$ or $p \mid M$. The latter condition is

$$(L^2 + 27M^2 - 4) \mid 24M\,,$$

giving $M = 1$ and hence $(L^2 + 23) \mid 24$. So $L = 1$ and $p = 1$, which is impossible.

The former condition is

$$(L^2 + 27M^2 - 4) \mid 24L$$

giving $L < 24$ and then also $M < 6$, thus $p \leq \frac{1}{24}(23^2 + 27 \cdot 5^2) = 50$. A computer check with C (testing the 6-Germain primes p up to 50) showed that $p \mid L$ only holds for $p = 23$.

Example 7. *The 6-Germain prime $p = 23$ is not a primitive root modulo 139. And indeed we have $L = 23$ and $M = 1$, thus $p \mid LM$.*

The remaining condition from Lehmer's theorem. Consider the condition

$$L \equiv \pm\frac{9r}{2u+1}M \bmod p \tag{2}$$

where

$$u \not\equiv 0, 1, -\frac{1}{2}, -\frac{1}{3} \bmod p \quad \text{and} \quad 3u + 1 \equiv r^2(3u - 3) \bmod p\,.$$

The last congruence is equivalent to

$$u \equiv \frac{3r^2 + 1}{3(r^2 - 1)} \bmod p$$

recalling that p is coprime to 3 and that $r^2 \not\equiv 1$ (else the given congruence would imply $p \mid 4$). Excluding the listed values for $(u \bmod p)$ means excluding those values of r such that at least one of the following holds:

$$3r^2 + 1 \equiv 0 \bmod p \qquad 3r^2 + 1 \equiv 3(r^2 - 1) \bmod p$$
$$-2(3r^2 + 1) \equiv 3(r^2 - 1) \bmod p \qquad -3(3r^2 + 1) \equiv 3(r^2 - 1) \bmod p\,.$$

We then need to exclude r^2 equivalent to $-\frac{1}{3}$, $\frac{1}{9}$, or 0 modulo p.

Proof of Theorem 2. We can prove the theorem by hand for $p = 3$ (it is a primitive root modulo 19; we have $p \equiv 3 \bmod 4$ and there is no r satisfying (1) modulo 3 with $L = 7$ and $M = 1$), for $p = 5$ (it is not a primitive root modulo 31; we don't have $p \equiv 3 \bmod 4$), for $p = 23$ (it is not a primitive root modulo 139; the congruence (1) modulo 23 with $L = 23$ and $M = 1$ is satisfied with $r = 0$). Now we may suppose that $p > 7$ and $p \neq 23$.

We make use of the considerations made in this section, observing that we can rewrite (2) as (1). Now we inspect the excluded values of r for (2). We remark that for $r^2 \equiv 0 \bmod p$ the congruence (1) does not hold (because we have shown that $p \nmid L$), so we do not need to exclude this value. The same holds for $r^2 \equiv -\frac{1}{3} \bmod p$ because in this case the congruence can be rewritten as

$$L \equiv \pm 9rM^2 \bmod p$$

hence

$$L^2 \equiv -27M^2 \bmod p$$

implying that

$$4 \equiv 4q \equiv L^2 + 27M^2 \equiv 0 \bmod p\,,$$

which is impossible because $p > 7$. □

Example 8. *The 6-Germain prime $p = 11$ is a primitive root modulo 67: we have $p \equiv 3 \bmod 4$ and $L = 5$ and $M = 3$, and the congruence*

$$5 \equiv \pm\frac{27r(r^2-1)}{9r^2-1}3 \bmod 11$$

is not satisfied for any $r \in \mathbb{Z}$.

Example 9. *The 6-Germain prime $p = 83$ is not a primitive root modulo 499: we have $p \equiv 3 \bmod 4$ and $L = 32$ and $M = 6$, and the congruence*

$$32 \equiv \frac{27r(r^2-1)}{9r^2-1}6 \bmod 83$$

is satisfied for example taking $r = 3$.

References

[1] A. Ecker, *On primitive roots*, Elem. Math. 37, 103-108 (1982).

[2] R. Fueter, *Über primitive Wurzeln von Primzahlen*, Comment. Math. Helv. 18, 217-223 (1946).

[3] E. Lehmer *Criteria for Cubic and Quartic Residuacity*, Mathematika, Lond. 5, 20-29 (1958).

[4] V.P. Ramesh and M. Makeshwari, *A Prime Primitive Root p of $2p+1$ is a Sophie Germain Prime*, Am. Math. Mon. 129, No. 6, 538 (2022).

[5] V.P. Ramesh and M. Makeshwari, *A Note on Generalized Sophie Germain Primes*, Reson. 28, 923–928 (2023).

[6] G. Wertheim, *Primitive Wurzeln der Primzahlen von der Form $2^x q^\lambda + 1$, in welcher $q = 1$ oder eine ungerade Primzahl ist*, Acta Math. 20, 143-152 (1896).

[7] Wikipedia contributors, *Cubic reciprocity*, Wikipedia, The Free Encyclopedia. Retrieved May 10, 2025, `https://en.wikipedia.org/w/index.php?title=Cubic_reciprocity&oldid=1215675848`.