COUNTING TAMELY RAMIFIED EXTENSIONS OF LOCAL FIELDS UP TO ISOMORPHISM

JIM BROWN, ROBERT CASS, KEVIN JAMES, RODNEY KEATON, SALVATORE PARENTI, AND DANIEL SHANKMAN

Abstract. Let p be a prime number and let K be a local field of residue characteristic p. In this paper we give a formula that counts the number of degree n tamely ramified extensions of K in the case p is of order 2 modulo n.

1. Introduction

Let $n > 1$ and p a prime with $p \nmid n$. Let K be a local field of residue characteristic p. In this paper we are interested in counting up to isomorphism the number of degree n tamely ramified extensions of K; we denote this number by $\mathcal{K}(n, p)$.

Let $e \mid n$ be a ramification index and set $f = n/e$ to be the residue class degree. Set $g_e = \gcd(e, p^f - 1)$. It is well-known that up to isomorphism the number of degree n ramification index e extensions of K is exactly the number of orbits of $\mathbb{Z}/g_e\mathbb{Z}$ under the action of p. We denote this number by $\mathcal{O}(e, p)$. We use this result to calculate the number of extensions by first calculating the size of orbits under this action.

In section 2 we present two straightforward cases where the orbit structure is easy to write down. In the following section we deal with determining the orbit structure of $\mathbb{Z}/g\mathbb{Z}$ under the action of p when p has order ℓ modulo g where ℓ is a prime. Finally, in section 4 we use the orbit counts to give our formulas for the number of tamely ramified extensions of K of degree n when p has order 2 modulo n.

In this paper we adopt the following notation. We will denote an orbit in $\mathbb{Z}/g\mathbb{Z}$ containing a under multiplication by p by $O_g(a, p)$. We denote the order of p in $(\mathbb{Z}/g\mathbb{Z})^\times$ by $\mathrm{ord}_g(p)$. We write $\mathrm{val}_\ell(n) = m$ if $\ell^m \mid\mid n$.

2. A couple of straightforward cases

We now give the two simplest cases, namely when $p \equiv \pm 1 \pmod{n}$.

Proposition 1. *Let $p \equiv 1 \pmod{n}$. Then we have $\mathcal{K}(n, p) = \sigma_1(n)$ where we recall*

$$\sigma_1(n) = \sum_{e \mid n} e.$$

Proof. Let $e \mid n$. Note that since $p \equiv 1 \pmod{n}$, we have $p \equiv 1 \pmod{e}$ so $p^{n/e} - 1 \equiv 0 \pmod{e}$. Thus, $g_e = \gcd(e, p^{n/e} - 1) = e$. Since $p \equiv 1 \pmod{e}$, multiplication by p sorts $\mathbb{Z}/e\mathbb{Z}$ into e distinct orbits. Thus, $\mathcal{O}(e,p) = e$. This gives the result. □

Proposition 2. *Let $p \equiv -1 \pmod{n}$. Then we have*

$$\mathcal{K}(n,p) = \sigma_0(n)$$

if n is odd and

$$\mathcal{K}(n,p) = \sum_{\substack{e \mid n \\ \mathrm{val}_2(e)=0}} \left(\frac{e+1}{2}\right) + \sum_{\substack{e \mid n \\ 0<\mathrm{val}_2(e)<\mathrm{val}_2(n)}} \left(\frac{e}{2}+1\right) + \sum_{\substack{e \mid n \\ \mathrm{val}_2(e)=\mathrm{val}_2(n)}} 2$$

if n is even.

Proof. First, suppose that n is odd and let $e \mid n$. Since n is odd, so is e and hence so is n/e. This gives

$$\begin{aligned} p^{n/e} - 1 &\equiv (-1)^{n/e} - 1 \pmod{e} \\ &\equiv -2 \pmod{e}, \end{aligned}$$

i.e., $p^{n/e} + 1 \equiv 0 \pmod{d}$ for every divisor $d \mid e$. However, this means if $g_e = \gcd(e, p^{n/e} - 1) > 1$, we must have some $d \mid e$ so that $d \mid p^{n/e} - 1$. This implies $d \mid p^{n/e} - 1$ and $d \mid p^{n/e} + 1$, i.e., $d \mid 2$. However, this is impossible since n is odd. Thus, $g_e = 1$ for every $e \mid n$. Thus, $\mathcal{O}(e,p) = 1$ for every e and so the number of extensions is exactly the number of divisors of n, i.e., $\mathcal{K}(n,p) = \sigma_0(n)$.

Consider the case now when $n = 2^m p_1^{m_1} \cdots p_r^{m_r}$ with $m > 0$. Let $e \mid n$ with $\mathrm{val}_2(e) < m$. Then we have n/e is even and so $p^{n/e} \equiv 1 \pmod{n}$, which gives $p^{n/e} \equiv 1 \pmod{e}$. Thus, $e \mid p^{n/e} - 1$ and so $g_e = \gcd(e, p^{n/e} - 1) = e$. Let $a \in \mathbb{Z}/e\mathbb{Z}$. If $0 < a < e/2$, then $2a < e$ and so $2a \not\equiv 0 \pmod{e}$. Thus, $pa \not\equiv a \pmod{e}$ and so $\#O_e(a,p) = 2$. If $e/2 < a < e$ then $e < 2a < 2e$, so $2a \not\equiv 0 \pmod{e}$ and so $pa \not\equiv a \pmod{e}$ and so $\#O_e(a,p) = 2$. If $e/2$ is an integer, then $\#O_e(e/2, p) = 1$. Thus, in this case the numbers of orbits of $\mathbb{Z}/e\mathbb{Z}$ under the action of p is given by

$$\mathcal{O}(e,p) = \begin{cases} \frac{e}{2}+1 & e \text{ even} \\ \frac{e+1}{2} & e \text{ odd.} \end{cases}$$

The contribution from these cases to the total number of extensions is given by

$$\sum_{\substack{e \mid n \\ \mathrm{val}_2(e)=0}} \left(\frac{e+1}{2}\right) + \sum_{\substack{e \mid n \\ 0<\mathrm{val}_2(e)<m}} \left(\frac{e}{2}+1\right).$$

The remaining case to deal with is when $\mathrm{val}_2(e) = m$. Here we have n/e is odd, so $p^{n/e} \equiv -1 \pmod{e}$. Thus, $p^{n/e} - 1 \equiv -2 \pmod{e}$ and so $p^{n/e} - 1$

cannot have any odd prime divisors in common with e. However, if $2^k \mid p^{n/e} - 1$, then we have

$$\begin{aligned} 0 &\equiv p^{n/e} - 1 \pmod{2^k} \\ &\equiv -2 \pmod{2^k}. \end{aligned}$$

This can happen only if $k = 1$, so $g_e = 2$ in this case. Since $p \equiv 1 \pmod 2$, this gives p splits $\mathbb{Z}/2\mathbb{Z}$ into 2 distinct orbits. Thus, we obtain

$$\sum_{\substack{e \mid n \\ \mathrm{ord}_2(e) = m}} 2$$

extensions from this case. Combining all of these gives the result. □

Unfortunately, even the next easiest case of n being square-free and p being of order 2 is quite a bit more complicated and one does not get nearly as nice of a formula as one gets in the case $p \equiv \pm 1 \pmod n$. In the next section we give the necessary orbit counting results to be able to generalize these results.

3. Counting orbits

In this section we present results on counting orbit sizes that will be necessary to generalize the cases presented in the previous section. This section provides the heart of the paper.

Throughout this section we write $g = 2^m p_1^{m_1} \cdots p_r^{m_r}$ with $m \geq 0$, $m_i \geq 1$, and the p_i odd distinct primes.

Lemma 3. *Let* $\mathrm{ord}_g(p) = k$. *Then for any* $a \in \mathbb{Z}/g\mathbb{Z}$ *we have* $\#O_g(a,p) \leq k$.

Proof. We have $O_g(a,p) \subset \{a, pa, p^2a, \ldots, p^{k-1}a\}$, which gives the result. □

Lemma 4. *Let* $a \in (\mathbb{Z}/g\mathbb{Z})^\times$ *and let* $\mathrm{ord}_g(p) = k$. *Then* $\#O_g(a,p) = k$.

Proof. We know that $\#O_g(a,p) \leq k$ by the first claim. Suppose that $\#O_g(a,p) < k$. Then there exists $1 \leq j < k$ so that $p^j a = a$. However, since a is a unit this is equivalent to $p^j = 1$, which contradicts $\mathrm{ord}_g(p) = k$. □

We begin with the case that $g = 2^m$ and $\mathrm{ord}_g(p) = 2$. Clearly if $g = 2$ there are exactly 2 orbits. If $g = 4$, then the only element of order 2 is 3, and this falls under what we have done above as $3 \equiv -1 \pmod 4$, so the orbits are size 2 if $a = 1, 3$ and size 1 if $a = 0, 2$. We can now assume $m \geq 3$. We claim there are exactly 3 elements of order 2 in $(\mathbb{Z}/2^m\mathbb{Z})^\times$ and they are given by $-1, 2^{m-1} \pm 1$. To see there are three elements of order 2, recall that $(\mathbb{Z}/2^m\mathbb{Z})^\times \cong Z_2 \times Z_{2^{m-2}}$ where Z_n is a cyclic group of order n. Let x be the unique element of order 2 in Z_2 and let y be the unique element of order 2 in $Z_{2^{m-2}}$. Then the only elements of order 2 are given by $(x,y), (1,y)$, and

$(x, 1)$. It is now simple to see the elements claimed have order 2 by using the fact that $m \geq 3$ so

$$\begin{aligned}(2^{m-1} \pm 1)^2 &= 2^{2m-2} \pm 2^m + 1 \\ &\equiv 2^m 2^{m-2} + 1 \pmod{2^m} \\ &\equiv 1 \pmod{2^m}.\end{aligned}$$

Thus, we only need consider these three elements when determining the orbit structure. We already know if $p \equiv -1 \pmod{2^m}$, then the orbits have size 2 except for $a = 0, 2^{m-1}$. Let $p \equiv 2^{m-1} - 1 \pmod{2^m}$. If $a = 2^{m-1}$, we have

$$\begin{aligned}pa &= 2^m 2^{m-2} - 2^{m-1} \\ &\equiv -2^{m-1} \pmod{2^m} \\ &\equiv a \pmod{2^m}.\end{aligned}$$

Thus, $a = 0, 2^{m-1}$ have orbits of size 1. We know all odd a have orbits of size 2, so it remains to deal with the case that $a = 2^j b$ for $1 \leq j < m - 1$ and b odd. If $pa \equiv a \pmod{2^m}$, then using that b is a unit modulo 2^m we have

$$(2^{m-1} - 1)2^j \equiv 2^j \pmod{2^m}$$

which is equivalent to $m \mid (m-2)$. However, this is impossible since $m \geq 3$. Thus, unless $a = 0, 2^{m-1}$ we have $\#O_{2^m}(a, p) = 2$. It now only remains to deal with $p \equiv 2^{m-1}+1 \pmod{2^m}$. Here we claim $\#O_{2^m}(a, p) = 1$ unless a is odd. We have that if a is odd then the orbit size is size 2, so it only remains to show that if a is even it is its own orbit. This is easy as $(2^{m-1}+1)2j \equiv 2j \pmod{2^m}$. Thus, we have shown the following.

Lemma 5. *Let $m \geq 1$ and set $g = 2^m$. Let p be an odd prime with $\mathrm{ord}_{2^m}(p) = 2$. We have the following orbit structure of $\mathbb{Z}/g\mathbb{Z}$ under the action of p:*

1. *if $m = 1$, there are two orbits each of size 1;*
2. *if $m = 2$, there are two orbits of size 1 ($\{0\}, \{2\}$) and one orbit of size 2 ($\{1,3\}$);*
3. *if $m \geq 3$, then we split into cases:*
   (a) *if $p \equiv -1 \pmod{2^m}$, then all orbits have size 2 except $\{0\}$ and $\{2^{m-1}\}$ are their own orbits;*
   (b) *if $p \equiv 2^{m-1} - 1 \pmod{2^m}$, then all orbits have size 2 except $\{0\}$ and $\{2^{m-1}\}$ are their own orbits;*
   (c) *if $p \equiv 2^{m-1}+1 \pmod{2^m}$, then if a is even $\{a\}$ is its own orbit, and otherwise the orbit has size 2.*

The next case to deal with is when $\mathrm{ord}_g(p) = \ell$, ℓ a prime, and if $\ell^{m_\ell} \mid\mid g$ then $\mathrm{ord}_{\ell^{m_\ell}}(p) = 1$. Observe the last requirement gives that in order to have an element p of order ℓ modulo g, it must be the case that $\ell \mid (p_i - 1)$ for some $i = 1, \ldots, r$. We will make use of the following fact in the proof of Lemma 7.

Lemma 6. *Suppose* $\mathrm{ord}_g(p) = \ell$ *where* ℓ *is a prime and assume if* $\ell^{m_\ell} \mid\mid g$ *then* $\mathrm{ord}_{\ell^{m_\ell}}(p) = 1$. *If* $\mathrm{ord}_{p_i^{m_i}}(p) = \ell$, *then* $\mathrm{ord}_{p_i}(p) = \ell$.

Proof. Our assumption implies that $\ell \mid (p_i - 1)$. Suppose that it is the case that $\mathrm{ord}_{p_i}(p) = 1$. Set $D = (p_i - 1)p_i^{m_i - 1}$ and observe we have a commutative diagram where θ is the natural projection map taking $a \pmod{p_i^{m_i}}$ to $a \pmod{p_i}$, Z_D and Z_{p_i-1} are cyclic groups, and if we write $Z_D = \langle x \rangle$, then ϕ is the map that sends x to $x^{p_i^{m_i-1}}$, which is a generator of Z_{p_i-1}.

$$\begin{array}{ccc} (\mathbb{Z}/p_i^{m_i}\mathbb{Z})^\times & \xrightarrow{\cong} & Z_D \\ \Big\downarrow{\scriptstyle \theta} & & \Big\downarrow{\scriptstyle \phi} \\ (\mathbb{Z}/p_i\mathbb{Z})^\times & \xrightarrow{\cong} & Z_{p_i-1} \end{array}$$

Since p has order ℓ in $(\mathbb{Z}/p_i^{m_i}\mathbb{Z})^\times$, it necessarily corresponds to an element of the form $x^{aD/\ell}$ for some $0 < a < \ell$. However, we have that $\phi(x^{aD/\ell}) \neq 1$ in Z_{p_i-1} because we cannot have $p_i - 1 \mid \frac{aD}{\ell}$ since $\mathrm{val}_\ell\left(\frac{p_i^{m_i-1}aD}{\ell}\right) < \mathrm{val}_\ell(p_i - 1)$ as $\ell \nmid p_i a$. This contradicts the fact that we are assuming $\theta(p) = 1$. □

Lemma 7. *Suppose* $\mathrm{ord}_g(p) = \ell$ *where* ℓ *is a prime and assume if* $\ell^{m_\ell} \mid\mid g$ *then* $\mathrm{ord}_{\ell^{m_\ell}}(p) = 1$. *Let* $a \in \mathbb{Z}/g\mathbb{Z}$. *If* $\gcd(a, g) = 1$, *then* $\#O_g(a, p) = \ell$. *Now suppose* $\gcd(a, g) > 1$. *Let* $\mathcal{P} = \prod_j p_j^{m_j}$ *so that* $\mathrm{ord}_{p_j^{m_j}}(p) = \ell$. *If* $\mathcal{P} \mid a$ *then* $\#O_g(a, p) = 1$. *If* $\mathcal{P} \nmid a$ *we have* $\#O_g(a, p) = \ell$.

Proof. We have already covered the case $\gcd(a, g) = 1$.

Assume now that $\mathcal{P} \mid a$. The claim is that $\#O_g(a, p) = 1$. Let $\mathcal{Q} = g/\mathcal{P}$. We use the isomorphism $\mathbb{Z}/g\mathbb{Z} \cong \mathbb{Z}/\mathcal{P}\mathbb{Z} \times \mathbb{Z}/\mathcal{Q}\mathbb{Z}$ to write $p = (p_\mathcal{P}, p_\mathcal{Q})$ and $a = (a_\mathcal{P}, a_\mathcal{Q})$. Note that $\mathrm{ord}_\mathcal{P}(p_\mathcal{P}) = \ell$ and $\mathrm{ord}_\mathcal{Q}(p_\mathcal{Q}) = 1$ by construction of $\mathcal{P}$ and $\mathcal{Q}$. Moreover, we have $a_\mathcal{P} = 0$ by assumption. Since $\mathrm{ord}_\mathcal{Q}(p_\mathcal{Q}) = 1$, we have $pa = (p_\mathcal{P}, p_\mathcal{Q}) \cdot (0, a_\mathcal{Q}) = (p_\mathcal{P} \cdot 0, p_\mathcal{Q} \cdot a_\mathcal{Q}) = (0, a_\mathcal{Q}) = a$. Thus, $O_g(a, p) = \{a\}$, as claimed.

Now suppose that $\mathcal{P} \nmid a$. We need to show that $p^j a \neq a \pmod{g}$ for $1 \leq j < \ell$. Suppose that there is such a j, namely, we have $p^j a = a \pmod{g}$. We can rewrite this as $(p_\mathcal{P}^j a_\mathcal{P}, p_\mathcal{Q}^j a_\mathcal{Q}) = (a_\mathcal{P}, a_\mathcal{Q})$, i.e., $p_\mathcal{P}^j a_\mathcal{P} = a_\mathcal{P}$ and $p_\mathcal{Q}^j a_\mathcal{Q} = a_\mathcal{Q}$. Using the first of these equations, we have $p_\mathcal{P}^j a_\mathcal{P} - a_\mathcal{P} = 0$, i.e., $a_\mathcal{P}(p_\mathcal{P}^j - 1) = 0$. However, this gives that $p_i \mid (p_\mathcal{P}^j - 1)$ for some $p_i \mid \mathcal{P}$ for otherwise $\mathcal{P} \mid a$, i.e., p has order less than ℓ modulo p_i. However, this contradicts Lemma 6 and the assumption that $p_i \mid \mathcal{P}$. Thus, we have $\#O_g(a, p) = \ell$ in this case. □

It is now elementary to combine Lemma 5 and Lemma 7 to get the general result when $\mathrm{ord}_p(g) = 2$.

Proposition 8. *Let p be a prime with $\mathrm{ord}_g(p) = 2$. Let $\mathcal{P}' = \prod_j p_j^{m_j}$ so that $\mathrm{ord}_{p_j^{m_j}}(p) = 2$. If $\mathrm{ord}_{2^m}(p) = 1$, set $\mathcal{P} = \mathcal{P}'$. If $\mathrm{ord}_{2^m}(p) = 2$, then define $\mathcal{P}$ as follows:*

(1) *if $p \equiv -1 \pmod{2^m}$ or $p \equiv 2^{m-1} - 1 \pmod{2^m}$, set $\mathcal{P} = 2^{m-1}\mathcal{P}'$;*
(2) *if $p \equiv 2^{m-1} + 1 \pmod{2^m}$, set $\mathcal{P} = 2\mathcal{P}'$.*

If $\mathcal{P} \mid a$, then $\#O_g(a, p) = 1$. Otherwise, $\#O_g(a, p) = 2$.

Proof. The proof of this proposition amounts to combining Lemma 7 and Lemma 5. We have $\#O_g(a, p) = 2$ unless $\#O_{2^m}(a, p) = 1$ and $\#O_{p_i^{m_i}}(a, p) = 1$ for all i. However, these orbits all have size one exactly when $\mathcal{P} \mid a$ by the previous lemmas. □

Example 9. Let $g = 24$ so $m = 3$, $p_1 = 3$, and $m_1 = 1$. Consider the prime $p = 5$. Observe that p has order 2 modulo 24, modulo 3, and modulo 8. Moreover, $p = 2^{m-1}+1$. One easily checks that when acting upon $\mathbb{Z}/24\mathbb{Z}$ by 5, the orbits are given by $\{0\}$, $\{1, 5\}$, $\{2, 10\}$, $\{3, 15\}$, $\{4, 20\}$, $\{6\}$, $\{7, 11\}$, $\{8, 16\}$, $\{9, 21\}$, $\{12\}$, $\{13, 17\}$, $\{14, 22\}$, $\{18\}$, and $\{19, 23\}$, which agrees with the proposition since in this case $\mathcal{P} = 6$.

Though it will not be used in our counting arguments, it is now easy to provide the analogous result to Proposition 8 for the case $\mathrm{ord}_g(p) = \ell$ for ℓ an odd prime. We provide this result for completeness. The next step is to deal with the case when $\mathrm{ord}_g(p) = \ell$ for ℓ an odd prime with $\ell \mid g$ but $\ell \nmid (p_j - 1)$ for all $j = 1, \ldots, r$. Note for this to be possible we must have $\ell = p_i$ for some i with $m_i > 1$.

Lemma 10. *Let p be a prime with $\mathrm{ord}_g(p) = p_i$ for some $i = 1, \ldots, r$ and assume $p_i \nmid (p_j - 1)$ for all $j = 1, \ldots, r$. Let $a \in \mathbb{Z}/g\mathbb{Z}$. If $p_i \mid a$ then $\#O_g(a, p) = 1$. Otherwise $\#O_g(a, p) = p_i$.*

Proof. Without loss of generality we can assume $\mathrm{ord}_g(p) = p_1$. Write $h = g/p_1^{m_1}$. We can write $\mathbb{Z}/g\mathbb{Z} \cong \mathbb{Z}/p_1^{m_1}\mathbb{Z} \times \mathbb{Z}/h\mathbb{Z}$. Since $p_1 \nmid \varphi(h)$ by assumption, we have $\mathrm{ord}_h(p) = 1$ and so p acts as the identity on $\mathbb{Z}/h\mathbb{Z}$.

Suppose that $p_1 \nmid a$ and assume there is a j with $1 \leq j < p_1$ so that $p^j a \equiv a \pmod{g}$. Since p acts trivially on $\mathbb{Z}/h\mathbb{Z}$, this statement is equivalent to $p^j a_{p_1^{m_1}} = a_{p_1^{m_1}}$ for some j with $1 \leq j < p_1$. However, this gives $p_1^{m_1} \mid (p^j - 1)$, which contradicts the fact that p necessarily has order p_1 modulo $p_1^{m_1}$. Thus, it must be that if $p_1 \nmid a$, then $\#O_g(a, p) = \ell$.

Now assume $p_1 \mid a$ and write $a = p_1 c$. Again we use the fact that p acts as the identity on $\mathbb{Z}/h\mathbb{Z}$ to conclude we only need to determine what happens to the $p_1^{m_1}$ component of a. Here we make use of the fact that if p has order p_1 in $\mathbb{Z}/p_1^{m_1}\mathbb{Z}$, then $p = bp_1^{m_1-1} + 1$ for some $1 \leq b \leq p_1 - 1$. The result is then clear because we have $pa = (bp_1^{m_1-1} + 1)(p_1 c) = p_1 c = a$ in the $p_1^{m_1}$ component. □

We now combine Proposition 8 and Lemma 10 to obtain the following result.

Proposition 11. *Let p be a prime with $\mathrm{ord}_g(p) = \ell$ for ℓ an odd prime. Let $\mathcal{P}' = \prod_j p_j^{m_j}$ so that $\mathrm{ord}_{p_j^{m_j}}(p) = \ell$ and $\ell \neq p_j$. If $\ell \nmid g$, set $\mathcal{P} = \mathcal{P}'$. If $\ell = p_j$ for some $1 \leq j \leq m$ and $\mathrm{ord}_{p_j^{m_j}}(p) = c$, set $\mathcal{P} = c\mathcal{P}'$ where $c = 1, \ell$. If $\mathcal{P} \mid a$, then $\#O_g(a,p) = 1$. Otherwise, $\#O_g(a,p) = \ell$.*

Proof. Note that if $\ell \nmid g$ or $c = 1$ we are done, so assume without loss of generality that $\ell = p_1$ and $\mathrm{ord}_{\ell^{m_1}}(p) = \ell$. First suppose that $\mathcal{P} \mid a$. Set $\mathcal{Q} = g/\ell^{m_1}\mathcal{P}'$ and consider the isomorphism $\mathbb{Z}/g\mathbb{Z} \cong \mathbb{Z}/\ell^{m_1}\mathbb{Z} \times \mathbb{Z}/\mathcal{P}'\mathbb{Z} \times \mathbb{Z}/\mathcal{Q}\mathbb{Z}$. By assumption we can write $a = (a_{\ell^{m_1}}, a_{\mathcal{P}'}, a_{\mathcal{Q}}) = (a_{\ell^{m_1}}, 0, a_{\mathcal{Q}})$. Observe that we have

$$\begin{aligned} pa &= (pa_{\ell^{m_1}}, 0, pa_{\mathcal{Q}}) \\ &= (pa_{\ell^{m_1}}, 0, a_{\mathcal{Q}}) \quad (\text{since } \mathrm{ord}_{\mathcal{Q}}(p) = 1 \text{ by assumption}) \\ &= (a_{\ell^{m_1}}, 0, a_{\mathcal{Q}}) \quad (\text{by Lemma 10}) \\ &= a. \end{aligned}$$

Thus, if $\mathcal{P}$ divides a we have the orbit has size 1 as claimed. Now suppose $\mathcal{P} \nmid a$ but $p^j a = a$ for some $1 \leq j \leq \ell$. However, this leads to the equations $p^j a_{\ell^{m_1}} = a_{\ell^{m_1}}$ and $p^j a_{\mathcal{P}'} = a_{\mathcal{P}'}$. Since $\mathcal{P} \nmid a$ these cannot both hold from what we have done above unless $j = \ell$. □

Note that in the next section where g will vary we will write $\mathcal{P}_g$ to keep track of the group $\mathbb{Z}/g\mathbb{Z}$ upon which p is acting.

4. Main counting results

We are now able to give the formulas for counting the number of degree n tamely ramified extensions of K by using the orbit structure of $\mathbb{Z}/g\mathbb{Z}$ given in the previous section when p has order 2 modulo n. Throughout this section we write $n = 2^m p_1^{m_1} \cdots p_r^{m_r}$ with $m \geq 0$, $m_i \geq 1$, and the p_i distinct odd primes.

Consider the case that $\mathrm{val}_2(e) = m$. By assumption we have n/e is odd and so $p^{n/e} - 1 \equiv p - 1 \pmod{e}$. Thus, we have p splits $\mathbb{Z}/g_e\mathbb{Z}$ into g_e orbits and so we obtain the number of degree n extensions of K arising from this situation is given by

$$\sum_{\substack{e \mid n \\ \mathrm{val}_2(e) = \mathrm{val}_2(n)}} g_e$$

degree n extensions of K from this situation.

Now suppose that $\mathrm{val}_2(e) < m$. Then we have $2 \mid n/e$ and so $g_e = \gcd(e, p^{n/e} - 1) = \gcd(e, 0) = e$. It is not necessarily the case that $\mathrm{ord}_e(p) = 2$, so we break this into two cases. If $\mathrm{ord}_e(p) = 1$, then p acts on $\mathbb{Z}/e\mathbb{Z}$ as the identity so splits it into e distinct orbits. Thus, for this case we have $\mathcal{O}(e,p) = e$. If $\mathrm{ord}_e(p) = 2$, we can use Proposition 8 to count the orbits in

terms of $\mathcal{P}_e$. In this case we have the number of orbits given by

$$\mathcal{O}(e,p) = \frac{\varphi(e)}{2} + \frac{\#\left\{a \in \mathbb{Z}/e\mathbb{Z} : \gcd(a,e) > 1, a \neq 0, \mathcal{P}_e \nmid a\right\}}{2} + \#\left\{a \in \mathbb{Z}/e\mathbb{Z} : \gcd(a,e) > 1, a \neq 0, \mathcal{P}_e \mid a\right\} + 1$$

where the 1 comes from 0 always being its own orbit.

Combining all of this we have the following theorem.

Theorem 12. *Let p be a prime with with $p \nmid n$ and $\operatorname{ord}_p(n) = 2$. For $e \mid n$, define $\mathcal{P}_e$ as in Proposition 8. The number of degree n extensions of K up to isomorphism is given by*

$$\begin{aligned}\mathcal{K}(n,p) = &\sum_{\substack{e \mid n \\ \operatorname{val}_2(e) = \operatorname{val}_2(n)}} g_e + \sum_{\substack{e \mid n \\ \operatorname{val}_2(e) = 0 \\ p \equiv 1 \pmod{e}}} e \\ &+ \sum_{\substack{e \mid n \\ \operatorname{val}_2(e) = 0 \\ p \not\equiv 1 \pmod{e}}} \left(\frac{\varphi(e)}{2} + \frac{\#\left\{a \in \mathbb{Z}/e\mathbb{Z} : \gcd(a,e) > 1, a \neq 0, \mathcal{P}_e \nmid a\right\}}{2} \right) \\ &+ \sum_{\substack{e \mid n \\ \operatorname{val}_2(e) = 0 \\ p \not\equiv 1 \pmod{e}}} \left(\#\left\{a \in \mathbb{Z}/e\mathbb{Z} : \gcd(a,e) > 1, a \neq 0, \mathcal{P}_e \mid a\right\} + 1 \right).\end{aligned}$$

One can easily check that this result recovers Lemma 2 in the case we take $p \equiv -1 \pmod{n}$.

We note that while we have the relevant orbit counting results for p of prime order ℓ modulo n, it is not as straightforward to count the extensions in this case. In the case $\ell = 2$, when we consider $p^{n/e} - 1$ modulo e, this is either 0 if $\operatorname{val}_2(e) < m$ or $p - 1$ if $\operatorname{val}_2(e) = m$ due to the fact that the only remainders possible upon dividing n/e by 2 are 0 or 1. In either case it is easy to use the orbit structure to give a count. However, for general ℓ we must consider remainders $0, 1, \ldots, \ell - 1$. If the remainder is larger than 1, it

is not obvious how p will act on $\mathbb{Z}/g_e\mathbb{Z}$ in this case. This will be the subject of future research.

Department of Mathematical Sciences, Clemson University, Clemson, SC 29634
E-mail address: jimlb@clemson.edu

Department of Mathematics, University of Kentucky, Lexington, KY 40506
E-mail address: robert.cass@uky.edu

Department of Mathematical Sciences, Clemson University, Clemson, SC 29634
E-mail address: kevja@clemson.edu

Department of Mathematical Sciences, Clemson University, Clemson, SC 29634
E-mail address: rkeaton@clemson.edu

Department of Mathematics, University of Michigan, Ann Arbor, MI 48109
E-mail address: sparenti@umich.edu

Department of Mathematics, University of Tennessee, Knoxville, TN 37996
E-mail address: dshankma@utk.edu