COUNTING TAMELY RAMIFIED EXTENSIONS OF LOCAL FIELDS UP TO ISOMORPHISM

Jim Brown
Department of Mathematical Sciences, Clemson University, Clemson, SC 29634, USA
jimlb@g.clemson.edu

Robert Cass
Department of Mathematics, University of Kentucky, Lexington, KY 40506, USA
robert.cass@uky.edu

Kevin James
Department of Mathematical Sciences, Clemson University, Clemson, SC 29634, USA
kevja@clemson.edu

Rodney Keaton
Department of Mathematics, University of Oklahoma, Norman, OK 73019, USA
rkeaton@math.ou.edu

Salvatore Parenti
Department of Mathematics, University of Wisconsin, Madison, WI 53706, USA
sparenti@wisc.edu

Daniel Shankman
Department of Mathematics, Purdue University, West Lafayette, IN 47907, USA
dshankma@purdue.edu

Received: , Revised: , Accepted: , Published:

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

A central problem in number theory is to classify finite field extensions E/F for F a global field. As there are infinitely many such extensions for any fixed degree n, this is a difficult problem. It is often more tractable to instead classify local field extensions and use this information to study global field extensions. In particular, given a local field K of residue characteristic p, it is well known that up to isomorphism there are only finitely many extensions E/K of fixed degree n and so such classifications are tractable. In this paper we provide a formula for the number of degree n tamely ramified extensions of K in the case that p has order 2 modulo n. One can see Theorem 1 for a precise statement of the result.

The classification of finite extensions of local fields amounts to classifying unramified, tamely ramified, and wildly ramified extensions. Unramified extensions are easy to classify as there is only one such field extension for each fixed degree n. Classifying wildly ramified extensions is much more difficult and complete classifications are only known for small degrees (see for example [1, 2, 4]). In this paper we study the case of tamely ramified extensions, which falls between unramified and wildly ramified extensions in terms of difficulty.

Let $e \mid n$ be a ramification index and set $f = n/e$ to be the residue class degree. The number of degree n ramification index e extensions of K has been calculated by Roquette by studying defining polynomials for tamely ramified extensions over the inertia field of K. The reader is referred to [3, Chap. 16] for a description of these results. We take a different approach that relies only on elementary counting and group action arguments. Set $g_e = \gcd(e, p^{n/e} - 1)$. It is 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 ([3, Chap. 16]). We use elementary methods to calculate the size of the orbits of $\mathbb{Z}/g_e\mathbb{Z}$ under the action of p, and thus the number of degree n ramification index e extensions of K. We then use these orbit counts to provide a formula for the number of degree n tamely ramified extensions of K in the case that p has order 2 modulo n by summing over the number of orbits.

In section 2 we present two straightforward cases where the orbit structure is easy to write down. We then 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 denote the order of p in $(\mathbb{Z}/g\mathbb{Z})^\times$ by $\mathrm{ord}_g(p)$. We write $v_p(n) = m$ if $p^m \mid\mid n$. We will denote an orbit in $\mathbb{Z}/g\mathbb{Z}$ containing a under multiplication by p by $O_g(a, p)$. We let $\mathcal{K}(n, p)$ denote the number of degree n tamely ramified extensions of K up to isomorphism and $\mathcal{O}(e, p)$ the number of orbits of $\mathbb{Z}/g_e\mathbb{Z}$ under the action of p, where we recall from above

that $g_e = \gcd(e, p^{n/e} - 1)$, which will be used throughout. In particular, we have $\mathcal{K}(n,p) = \sum_{e|n} \mathcal{O}(e,p)$.

2. A couple of straightforward cases

We now give the two simplest cases, namely when $p \equiv \pm 1 \pmod{n}$. Given a non-negative integer k and a positive integer n, let $\sigma_k(n)$ denote the sum of the kth powers of the positive divisors of n, i.e.,

$$\sigma_k(n) = \sum_{d|n} d^k.$$

In particular, the function $\sigma_0(n)$ is simply the number of divisors of n (often denoted $\tau(n)$), and the function $\sigma_1(n)$ is simply the sum of divisors of n (often denoted $\sigma(n)$).

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

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, $g_e = e$. 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 $p \equiv -1 \pmod{n}$. We have*

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

if n is odd and

$$\mathcal{K}(n,p) = (m + 3/2)\sigma_0(m) + 2^{m-1}\sigma_1(m)$$

if n is even and we write $n = 2^m b$.

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 $g_e > 1$, we must have some $d > 1$ with $d \mid e$ 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 $v_2(e) < m$. This implies n/e is even and so $p^{n/e} \equiv 1 \pmod{n}$. In particular, we have $p^{n/e} \equiv 1 \pmod{e}$. Thus, $e \mid p^{n/e} - 1$ and so $g_e = e$. 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 hence $\#O_e(a,p) = 2$. If $e/2 < a < e$ then $e < 2a < 2e$, so $2a \not\equiv 0 \pmod{e}$. This implies $pa \not\equiv a \pmod{e}$ and thus $\#O_e(a,p) = 2$. 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

$$\sum_{\substack{e|n \\ v_2(e)=0}} \left(\frac{e+1}{2}\right) + \sum_{\substack{e|n \\ 0<v_2(e)<m}} \left(\frac{e}{2}+1\right).$$

The remaining case to deal with is when $v_2(e) = m$. 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 that p splits $\mathbb{Z}/2\mathbb{Z}$ into 2 distinct orbits. Thus, we obtain

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

extensions from this case. Combining all of these gives that

$$\mathcal{K}(n,p) = \sum_{\substack{e|n \\ v_2(e)=0}} \left(\frac{e+1}{2}\right) + \sum_{\substack{e|n \\ 0<v_2(e)<v_2(n)}} \left(\frac{e}{2}+1\right) + \sum_{\substack{e|n \\ v_2(e)=v_2(n)}} 2.$$

If we write $n = 2^m b$, then we have the following simplifications. We have

$$\begin{aligned} \sum_{\substack{e|n \\ v_2(e)=0}} \left(\frac{e+1}{2}\right) &= \sum_{e|b} \frac{e}{2} + \sum_{e|b} \frac{1}{2} \\ &= \frac{\sigma_1(b)}{2} + \frac{\sigma_0(b)}{2}, \end{aligned}$$

$$\sum_{\substack{e|n \\ 0<v_2(e)<v_2(n)}} \left(\frac{e}{2}+1\right) = \sum_{j=1}^{m-1} \sum_{e|b} \left(\frac{2^j e}{2}+1\right)$$
$$= \frac{1}{2}\sum_{j=1}^{m-1}\sum_{e|b} 2^j e + \sum_{j=1}^{m-1}\sum_{e|b} 1$$
$$= \frac{1}{2}\sum_{j=1}^{m-1} 2^j \sigma_1(b) + (m-1)\sigma_0(b)$$
$$= \left(\frac{2^m-1}{2}\right)\sigma_1(b) + (m-1)\sigma_0(b),$$

and

$$\sum_{\substack{e|n \\ v_2(e)=v_2(n)}} 2 = 2\sum_{e|b} 1$$
$$= 2\sigma_0(b).$$

Combining all of these gives the result. □

The next simplest case to study is where n is square-free and p is of order 2 modulo n. However, even this is quite a bit more complicated and one does not get nearly as clean of a formula as one gets in the previous case where $p \equiv \pm 1 \pmod{n}$.

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 are distinct odd primes.

Lemma 1. *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 $\#O_g(a,p) \leq k$ as $O_g(a,p) \subset \{a, pa, p^2a, \ldots, p^{k-1}a\}$. 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 $\mathrm{ord}_g(p) = k$. □

Lemma 2. *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.*

Proof. 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 $(\mathbb{Z}/2^m\mathbb{Z})^\times \cong C_2 \times C_{2^{m-2}}$ where C_n is a cyclic group of order n. Let x be the unique element of order 2 in C_2 and let y be the unique element of order 2 in $C_{2^{m-2}}$. 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 $(2^{m-1} + 1)2j \equiv 2j \pmod{2^m}$. □

We now return to the general case $g = 2^m p_1^{m_1} \cdots p_r^{m_r}$. 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 4.

Lemma 3. *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 $a \pmod{p_i}$, C_D and

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

C_{p_i-1} are cyclic groups, and if we write $C_D = \langle x \rangle$, then ϕ is the map that sends x to $x^{p_i^{m_i-1}}$, which is a generator of C_{p_i-1}.

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 $0 < a < \ell$. Note that we cannot have $p_i - 1 \mid \frac{aD}{\ell}$ since $v_\ell\left(\frac{p_i^{m_i-1}aD}{\ell}\right) < v_\ell(p_i - 1)$ as $\ell \nmid p_i a$. Thus, we must have that $\phi(x^{aD/\ell}) \neq 1$ in C_{p_i-1}. However, this contradicts the fact that we are assuming $\theta(p) = 1$. □

Lemma 4. *Suppose* $\mathrm{ord}_g(p) = \ell$ *where* ℓ *is a prime and assume if* $\ell^{m_\ell} \mid\mid g$ *then* $\mathrm{ord}_{\ell^{m_\ell}}(p) = 1$. *Set* $M = \prod_j p_j^{m_j}$ *so that* $\mathrm{ord}_{p_j^{m_j}}(p) = \ell$. *Let* $a \in \mathbb{Z}/g\mathbb{Z}$.

1. *If* $\gcd(a, g) = 1$, *then* $\#O_g(a, p) = \ell$.
2. *If* $\gcd(a, g) > 1$, *then:*
   (a) *if* $M \mid a$, *then* $\#O_g(a, p) = 1$;
   (b) *if* $M \nmid a$, *then* $\#O_g(a, p) = \ell$.

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

Assume now that $M \mid a$. The claim is that $\#O_g(a, p) = 1$. Let $N = g/M$. We use the isomorphism $\mathbb{Z}/g\mathbb{Z} \cong \mathbb{Z}/M\mathbb{Z} \times \mathbb{Z}/N\mathbb{Z}$ to write $p = (p_M, p_N)$ and $a = (a_M, a_N)$. Note that $\mathrm{ord}_M(p_M) = \ell$ and $\mathrm{ord}_N(p_N) = 1$ by construction of M and N. Moreover, we have $a_M = 0$ by assumption. Since $\mathrm{ord}_N(p_N) = 1$, we have $pa = (p_M, p_N) \cdot (0, a_N) = (p_M \cdot 0, p_N \cdot a_N) = (0, a_N) = a$. Thus, $O_g(a, p) = \{a\}$, as claimed.

Now suppose that $M \nmid a$. 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 $(p_M^j a_M, p_N^j a_N) = (a_M, a_N)$, i.e., $p_M^j a_M = a_M$ and $p_N^j a_N = a_N$. Using the first of these equations, we have $p_M^j a_M - a_M = 0$, i.e., $a_M(p_M^j - 1) = 0$. However, this gives that $p_i \mid (p_M^j - 1)$ for some $p_i \mid M$ for otherwise $M \mid a$, i.e., p has order less than ℓ modulo p_i. However, this contradicts Lemma 3 and the assumption that $p_i \mid M$. Thus, we have $\#O_g(a,p) = \ell$ in this case. □

We can now prove the general result when $\mathrm{ord}_p(g) = 2$.

Proposition 3. *Let p be a prime with $\mathrm{ord}_g(p) = 2$. Let $M' = \prod_j p_j^{m_j}$ so that $\mathrm{ord}_{p_j^{m_j}}(p) = 2$. If $\mathrm{ord}_{2^m}(p) = 1$, set $M = M'$. If $\mathrm{ord}_{2^m}(p) = 2$, then define M as follows:*

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

If $M \mid a$, then $\#O_g(a,p) = 1$. Otherwise, $\#O_g(a,p) = 2$.

Proof. The proof of this proposition amounts to combining Lemma 4 and Lemma 2. 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 $M \mid a$ by the previous lemmas. □

Example 1. *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 $M = 6$.*

Though it will not be used in our counting arguments, it is now easy to provide the analogous result to Proposition 3 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 5. *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 3 and Lemma 5 to obtain the following result.

Proposition 4. *Let p be a prime with $\mathrm{ord}_g(p) = \ell$ for ℓ an odd prime. Let $M' = \prod_j p_j^{m_j}$ so that $\mathrm{ord}_{p_j^{m_j}}(p) = \ell$ and $\ell \neq p_j$. If $\ell \nmid g$, set $M = M'$. If $\ell = p_j$ for some $1 \leq j \leq m$ and $\mathrm{ord}_{p_j^{m_j}}(p) = c$, set $M = cM'$ where $c = 1, \ell$. If $M \mid a$, 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 $M \mid a$. Set $N = g/\ell^{m_1} M'$ and consider the isomorphism $\mathbb{Z}/g\mathbb{Z} \cong \mathbb{Z}/\ell^{m_1}\mathbb{Z} \times \mathbb{Z}/M'\mathbb{Z} \times \mathbb{Z}/N\mathbb{Z}$. By assumption we can write $a = (a_{\ell^{m_1}}, a_{M'}, a_N) = (a_{\ell^{m_1}}, 0, a_N)$. Observe that we have

$$\begin{aligned} pa &= (pa_{\ell^{m_1}}, 0, pa_N) \\ &= (pa_{\ell^{m_1}}, 0, a_N) \quad (\text{since } \mathrm{ord}_N(p) = 1 \text{ by assumption}) \\ &= (a_{\ell^{m_1}}, 0, a_N) \quad (\text{by Lemma 5}) \\ &= a. \end{aligned}$$

Thus, if M divides a we have the orbit has size 1 as claimed. Now suppose $M \nmid a$ 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 $p^j a_{M'} = a_{M'}$. Since $M \nmid a$ these cannot both hold unless $j = \ell$. □

4. Main counting results

We are now able to state our main result. 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 $v_2(e) = m$. 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

$$\sum_{\substack{e|n \\ v_2(e)=v_2(n)}} g_e.$$

Now suppose that $v_2(e) < m$. Then we have $2 \mid n/e$ and so $g_e = \gcd(e, 0) = e$. 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, hence 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 3 to count the orbits in terms of M_e. (Note that since g varies in this section we write M_g to keep track of the group $\mathbb{Z}/g\mathbb{Z}$ upon which p is acting.) In this case we have the number of orbits given by

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

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

Combining all of this we obtain the following theorem.

Theorem 1. *Let p be a prime with $p \nmid n$ and $\mathrm{ord}_p(n) = 2$. For $e \mid n$, define M_e as in Proposition 3. The number of degree n extensions of K up to isomorphism is given by*

$$\mathcal{K}(n,p) = \sum_{\substack{e|n \\ v_2(e)=v_2(n)}} g_e + \frac{1}{2}\left(\sigma_1(n/2) + \sigma_1\left(\gcd\left(\frac{n}{2}, p-1\right)\right) + \sum_{\substack{e|\frac{n}{2} \\ e \nmid (p-1)}} \frac{e}{M_e}\right).$$

Proof. We immediately have from the preceding discussion that

$$\begin{aligned}\mathcal{K}(n,p) = &\sum_{\substack{e|n \\ v_2(e)=v_2(n)}} g_e + \sum_{\substack{e|n \\ v_2(e)<v_2(n) \\ p\equiv 1 \pmod e}} e \\ &+ \sum_{\substack{e|n \\ v_2(e)<v_2(n) \\ p\not\equiv 1 \pmod e}} \left(\frac{\varphi(e)}{2} + \frac{\#\left\{a \in \mathbb{Z}/e\mathbb{Z} : \gcd(a,e) > 1, a \neq 0, M_e \nmid a\right\}}{2}\right) \\ &+ \sum_{\substack{e|n \\ v_2(e)<v_2(n) \\ p\not\equiv 1 \pmod e}} \left(\#\left\{a \in \mathbb{Z}/e\mathbb{Z} : \gcd(a,e) > 1, a \neq 0, M_e \mid a\right\} + 1\right).\end{aligned}$$

First, we simplify the conditions underneath the sums. We note that $e|n; v_2(e) < v_2(n)$ is equivalent to $e|\frac{n}{2}$. We also note that $p \equiv 1 \pmod e$ is equivalent to $e|(p-1)$. Finally, in the last two sums we omit the condition that $a \neq 0$. In the first sum, note

that $\mathcal{P}_e \not| a \Rightarrow a \neq 0$. In the second sum we simply absorb the one to compensate. This gives the following expression.

$$\begin{aligned}\mathcal{K}(n,p) &= \sum_{\substack{e|n \\ v_2(e)=v_2(n)}} g_e + \sum_{\substack{e|\frac{n}{2} \\ e|(p-1)}} e \\ &+ \sum_{\substack{e|\frac{n}{2} \\ e\not|(p-1)}} \left(\frac{\phi(e)}{2} + \frac{\#\{a \in \mathbb{Z}/e\mathbb{Z} \ : \ \gcd(a,e) > 1; \mathcal{P}_e \not| a\}}{2} \right) \\ &+ \sum_{\substack{e|\frac{n}{2} \\ e\not|(p-1)}} \#\{a \in \mathbb{Z}/e\mathbb{Z} \ : \ \gcd(a,e) > 1; \mathcal{P}_e | a\}\end{aligned}$$

Now we note that the union of the two sets showing up in the last two sums along with the set of residue classes counted by $\phi(e)$ is just all of $\mathbb{Z}/e\mathbb{Z}$. We use this observation to rearrange the last two sums and obtain the following expression.

$$\begin{aligned}\mathcal{K}(n,p) = &\sum_{\substack{e|n \\ v_2(e)=v_2(n)}} g_e + \sum_{\substack{e|\frac{n}{2} \\ e|(p-1)}} e \\ &+ \frac{1}{2} \sum_{\substack{e|\frac{n}{2} \\ e\not|(p-1)}} (e + \#\{a \in \mathbb{Z}/e\mathbb{Z} \ : \ \gcd(a,e) > 1; M_e | a\}) \\ = &\sum_{\substack{e|n \\ v_2(e)=v_2(n)}} g_e + \frac{1}{2} \sum_{e|\frac{n}{2}} (e + \#\{a \in \mathbb{Z}/e\mathbb{Z} \ : \ \gcd(a,e) > 1; M_e | a\}) \\ &- \frac{1}{2} \sum_{e|\gcd\left(\frac{n}{2},(p-1)\right)} (\#\{a \in \mathbb{Z}/e\mathbb{Z} \ : \ \gcd(a,e) > 1; M_e | a\} - e)\end{aligned}$$

Note that

$$\#\{a \in \mathbb{Z}/e\mathbb{Z} \ : \ \gcd(a,e) > 1; M_e | a\} = \begin{cases} e - \phi(e) & \text{if } M_e = 1, \\ \frac{e}{M_e} & \text{otherwise.} \end{cases}$$

Since $M_e \neq 1$, we have $\#\{a \in \mathbb{Z}/e\mathbb{Z} \ : \ \gcd(a,e) > 1; M_e | a\} = \frac{e}{M_e}$.

Thus, we may write

$$\begin{aligned}\mathcal{K}(n,p) &= \sum_{\substack{e|n \\ v_2(e)=v_2(n)}} g_e \quad + \quad \frac{1}{2}\sum_{e|\frac{n}{2}}\left(e+\frac{e}{M_e}\right) - \frac{1}{2}\sum_{e|\gcd\left(\frac{n}{2},p-1\right)}\left(\frac{e}{M_e}-e\right) \\ &= \sum_{\substack{e|n \\ v_2(e)=v_2(n)}} g_e \quad + \quad \frac{1}{2}\left(\sigma_1(n/2)+\sigma_1(\gcd\left(\frac{n}{2},p-1\right)) + \sum_{\substack{e|\frac{n}{2} \\ e\nmid(p-1)}} \frac{e}{M_e}\right),\end{aligned}$$

which gives the result.

□

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

In the case $\ell = 2$, when we consider $p^{n/e}-1$ modulo e, this is either 0 if $v_2(e) < m$ or $p-1$ if $v_2(e) = m$ 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. Thus, 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. This will be the subject of future research.

Acknowledgments

The authors were partially supported by the grant NSF DMS-1156734 funding the Clemson REU on Computational algebraic geometry, combinatorics, and number theory during the summer of 2013. The authors would like to thank the referee for comments that improved the exposition of this paper.

References

[1] C. Awtrey. Dodecic 3-adic fields. *Int. J. Number Theory* **8** (2012), 933-944.

[2] J. Brown and R. Cass and R. Keaton and S. Parenti and D. Shankman. Degree 14 extensions of $\mathbb{Q}_7$. *Int. J. of Pure and Appl. Math.* **100(2)** (2015), 337-345.

[3] H. Hasse. *Number Theory*. Springer-Verlag. Berlin. 2002.

[4] J. Jones and D. Roberts. A database of local fields. *J. Symbolic Comput.* **41** (2006), 80-97.