WARING'S PROBLEM IN ALGEBRAIC NUMBER FIELDS

by

ALA' JAMIL ALNASER

M.S., Kansas State University, 2005

AN ABSTRACT OF A DISSERTATION

submitted in partial fulfillment of the
requirements for the degree

DOCTOR OF PHILOSOPHY

Department of Mathematics
College of Arts and Sciences

KANSAS STATE UNIVERSITY
Manhattan, Kansas
2009

Abstract

Let p be an odd prime and $\gamma(k,p^n)$ be the smallest positive integer s such that every integer is a sum of s k-th powers $\pmod{p^n}$. We establish $\gamma(k,p^n) \leq [k/2]+2$ and $\gamma(k,p^n) \ll \sqrt{k}$ provided that k is not divisible by $(p-1)/2$. Next, let $t=(p-1)/(p-1,k)$, and q be any positive integer. We show that if $\phi(t) \geq q$ then $\gamma(k,p^n) \leq c(q)k^{1/q}$ for some constant $c(q)$. These results generalize results known for the case of prime moduli. Next we generalize these results to a number field setting. Let F be a number field, R it's ring of integers and $\mathcal{P}$ a prime ideal in R that lies over a rational prime p with ramification index e, degree of inertia f and put $t=(p^f-1)/(p-1,k)$. Let $k=p^r k_1$ with $p \nmid k_1$ and $\gamma(k,\mathcal{P}^n)$ be the smallest integer s such that every algebraic integer in F that can be expressed as a sum of k-th powers $\pmod{\mathcal{P}^n}$ is expressible as a sum of s k-th powers $\pmod{\mathcal{P}^n}$. We prove for instance that when $p > e+1$ then $\gamma(k,\mathcal{P}^n) \leq c(t)p^{nf/\phi(t)}$. Moreover, if $p > e+1$ we obtain the upper bounds $\gamma(k,\mathcal{P}^n) \leq 2313\left(\frac{k}{k_1}\right)^{8.44/\log p}+\frac{1}{2}$ if $f=2$ or 3, and $\gamma(k,\mathcal{P}^n) \leq 129\left(\frac{k}{k_1}\right)^{5.55/\log p}+\frac{1}{2}$ if $f \geq 4$. We also show that if $\mathcal{P}$ does not ramify then $\gamma(k,\mathcal{P}^n) \leq \frac{17}{2}\left(\frac{k}{k_1}\right)^{2.83/\log p}+\frac{1}{2}$ if $f \geq 2$ and $k_1 \leq p^{f/2}$, and $\gamma(k,\mathcal{P}^n) \leq \left(\frac{f}{p^{f/2-1}}\right)k$ if $f > 2$ and $k_1 > p^{f/2}$.

WARING'S PROBLEM IN ALGEBRAIC NUMBER FIELDS

by

ALA' JAMIL ALNASER

M.S., Kansas State University, 2005

A DISSERTATION

submitted in partial fulfillment of the
requirements for the degree

DOCTOR OF PHILOSOPHY

Department of Mathematics
College of Arts and Sciences

KANSAS STATE UNIVERSITY
Manhattan, Kansas
2009

Approved by:

Major Professor
Todd Cochrane

Copyright

Abstract

Let p be an odd prime and $\gamma(k,p^n)$ be the smallest positive integer s such that every integer is a sum of s k-th powers $\pmod{p^n}$. We establish $\gamma(k,p^n) \leq [k/2]+2$ and $\gamma(k,p^n) \ll \sqrt{k}$ provided that k is not divisible by $(p-1)/2$. Next, let $t=(p-1)/(p-1,k)$, and q be any positive integer. We show that if $\phi(t) \geq q$ then $\gamma(k,p^n) \leq c(q)k^{1/q}$ for some constant $c(q)$. These results generalize results known for the case of prime moduli. Next we generalize these results to a number field setting. Let F be a number field, R it's ring of integers and $\mathcal{P}$ a prime ideal in R that lies over a rational prime p with ramification index e, degree of inertia f and put $t=(p^f-1)/(p-1,k)$. Let $k=p^r k_1$ with $p \nmid k_1$ and $\gamma(k,\mathcal{P}^n)$ be the smallest integer s such that every algebraic integer in F that can be expressed as a sum of k-th powers $\pmod{\mathcal{P}^n}$ is expressible as a sum of s k-th powers $\pmod{\mathcal{P}^n}$. We prove for instance that when $p > e+1$ then $\gamma(k,\mathcal{P}^n) \leq c(t)p^{nf/\phi(t)}$. Moreover, if $p > e+1$ we obtain the upper bounds $\gamma(k,\mathcal{P}^n) \leq 2313\left(\frac{k}{k_1}\right)^{8.44/\log p}+\frac{1}{2}$ if $f=2$ or 3, and $\gamma(k,\mathcal{P}^n) \leq 129\left(\frac{k}{k_1}\right)^{5.55/\log p}+\frac{1}{2}$ if $f \geq 4$. We also show that if $\mathcal{P}$ does not ramify then $\gamma(k,\mathcal{P}^n) \leq \frac{17}{2}\left(\frac{k}{k_1}\right)^{2.83/\log p}+\frac{1}{2}$ if $f \geq 2$ and $k_1 \leq p^{f/2}$, and $\gamma(k,\mathcal{P}^n) \leq \left(\frac{f}{p^{f/2-1}}\right)k$ if $f > 2$ and $k_1 > p^{f/2}$.

Table of Contents

Acknowledgments

The writing of a dissertation can be a lonely and isolating experience, yet it is obviously not possible without the personal and practical support of numerous people. Thus my sincere gratitude goes to Jesus Christ and the Holy Virgin Mary, my parents, my sisters, my brother, all my friends for their love, support, and patience over the last few years.

I wish to thank Professors Todd Cochrane, Chris Pinner, John Maginnis, Jennifer Paulhus and the Number Theory group of the Math Department at Kansas State University, for inspiring and encouraging me to pursue my studies.

My thanks go out to Fr. Daniel and Fr. Joseph and all the people of St. Mary Magdalene Orthodox Christian Mission in Manhattan, KS, for welcoming me so warmly.

Many people on the faculty and staff of K-State Math Department assisted and encouraged me in various ways during my course of studies. I am especially grateful to my Professors for all that they have taught me. And I thank the students whom I was privileged to teach and from whom I also learned much.

My graduate studies would not have been the same without the social and academic challenges and diversions provided by all my student-colleagues in the Math Department at KSU. I am particularly thankful to my friends Donald Adongo, Dmytro Shklyarov, Francois Petit and Mukta Bhandari.

Finally, this dissertation would not have been possible without the expert guidance of my esteemed advisor, Prof. Todd Cochrane. Not only was he readily available for me, as he so generously is for all of his students, but he always read and responded to the drafts of each chapter of my work more quickly than I could have hoped. Although he is not a man of many words, his oral and written comments are always extremely perceptive, helpful, and appropriate.

Dedication

This is dedicated to my father, mother, two sisters, brother and last but not least my advisor.

Chapter 1

Introduction.

The original problem as stated by Edward Waring in his book Meditationes Algebraicae (1770 edition, pages 203-204) was:

> "Omnis integer numerus vel est cubus; vel e duobus, tribus, $4, 5, 6, 7, 8$, vel novem cubus compositus: est etiam quadratoquadratus; vel e duobus, tribus et c. usque ad novemdecim compositus et sic deinceps." In the 1782 edition, page 349, he adds guardedly " .. . consimilia etiam afirmari possunt (exceptis excipiendis) de eodem numero quantitatum earundem dimensionum."

In modern language and notation, we call the previous statement "Waring's Problem", and we can state it as follows:

> "Can every positive integer be expressed as a sum of at most s k-th powers of positive integers, where s depends only on k, not on the number being represented?"

There seems to be little doubt that Waring had only limited numerical evidence in favor of his assertions and no shadow of a proof. The case $k = 2$ was proved by Lagrange in 1770, who showed that each positive integer could be expressed as a sum of at most four squares of positive integers. During the next 139 years, special cases of the problem were solved for $k = 3, 4, 5, 6, 7, 8, 10$. Finally in 1909 Hilbert [19] solved the problem for all k in a very

complicated argument, which did not produce an explicit bound or value for s. The minimal such is called "Waring's Number" and denoted by $\gamma(k)$.

Using their powerful *circle method*, Hardy and Littlewood [17] obtained a still deeper result containing Hilbert's theorem. They proved that for $a \in \mathbb{Z}$ the number $\Lambda(a)$ of rational integral solutions x_i (for $i = 1, 2, \ldots, s$) of the equation

$$x_1^k + x_2^k + \cdots + x_s^k = a$$

has the same order of magnitude as $a^{s/k-1}$. Namely,

$$\Lambda(a) = \frac{\Gamma^s(1+1/k)}{\Gamma(s/k)}\sigma a^{s/k-1} + o(a^{s/k-1})$$

where σ, the singular series, is a function of a, lying between finite positive bounds, see [27].

After spending a considerable amounts of time and effort on the problem, many variations of the problem emerged such as the case we discuss in Chapter 2. In the second chapter of this work we restrict our attention to finding upper bounds for Waring's Number modulo a positive integer m, denoted by $\gamma(k, m)$. We generalize many known results as well as develop new theorems.

The next logical step in the evolution of this problem is to direct the efforts towards studying the problem in Number Fields. Notice that not every integer can be represented as a finite sum of k-th powers. As an example, consider the sum of squares of Gaussian Integers

$$\begin{aligned}(a_1 + b_1 i)^2 + (a_2 + b_2 i)^2 + \cdots + (a_s + b_s i)^2 &= (a_1^2 + a_2^2 + \cdots + a_s^2 - b_1^2 - b_2^2 - \cdots - b_s^2) \\ &+ 2i(a_1 b_1 + a_2 b_2 + \cdots + a_s b_s).\end{aligned}$$

Clearly, any Gaussian integer with an odd imaginary part can not be expressed as a finite sum of squares of Gaussian integers.

Let F be any algebraic number field of degree $d = d_1 + 2d_2$, where d_1 is the number of real automorphisms and $2d_2$ is the number of complex automorphisms. Let R be the ring of integers of F, and k be a fixed positive integer. Let R_k be the subring of R generated by the

k-th powers of elements of R. An element of α in F is said to be *totally positive* if $\sigma(\alpha)$ is positive for all embeddings $\sigma : F \to \mathbb{R}$. $\Gamma_R(k)$ is defined to be the minimal positive integer s, such that any totally positive element in R_k of sufficiently large norm can be expressed as a sum of at most s k-th powers of totally positive elements in R.

Siegel [26] was the first to successfully find an upper bound for the number of squares one would need to express algebraic integers as a sum of squares, for those algebraic integers that can be expressed as a sum of squares. Later in [27] he developed a generalization of the Hardy-Littlewood method for Number Fields. Siegel obtained

$$\Gamma_R(k) \leq dk(2^{k-1} + d) + 1,$$

where d is the degree of the field extension $\mathbb{Q} \subseteq F$. He also posed the question "Is there a bound for $\Gamma_R(k)$ which is independent of the degree of the extension?".

Birch was among the first to answer Siegel's call. He proved in [5] that if $s \geq 2^k + 1$ and α is any totally positive algebraic integer with a sufficiently large norm, and if α is congruent to a sum of s k-th powers modulo any prime power, then α is the sum of at most s k-th powers of totally positive integers in R. That is,

$$\Gamma_R(k) \leq \max\{2^k + 1, \gamma_R(k, \mathcal{P}^n)\}, \tag{1.1}$$

where $\mathcal{P}^n$ runs through all prime power ideals in R. Note that $\gamma_R(k, \mathcal{P}^n)$ here is defined to be the minimal positive integer s, such that any element of R that can be expressed as a sum of k-th powers is the sum of at most s k-th powers of elements in $R \pmod{\mathcal{P}^n}$

Finding upper bounds for $\gamma_R(k, \mathcal{P}^n)$ is what we will refer to as "The Local Waring's Problem over Number Fields". Birch obtained an upper bound for the local case in [6]

$$\gamma_R(k, \mathcal{P}^n) \leq k^{16k^2}, \tag{1.2}$$

for all prime power ideals in R.

Ramanujam independently obtained in [24] the upper bound

$$\gamma_R(k, \mathcal{P}^n) \leq 8k^5. \tag{1.3}$$

for all prime power ideals in R.

In Chapter 3 of this work, we generalize some of the results that we obtain for the case of Waring's number modulo an integer m to the Number Field setting. In Chapter 4, we consider a slightly different approach to the Local Problem and we obtain upper bounds for $\gamma_R(k, \mathcal{P}^n)$ which are independent of the degree of the extension of the Number Field F, as well as consider the case when the prime ideal $\mathcal{P}$ does not ramify.

For more on the classical Waring's problem and other special cases see "Waring's Problem: A Survey" by R. C. Vaughan and T. D. Wooley [33].

Chapter 2

Waring's Number (mod m).

2.1 Introduction and Notation.

We start by considering "Waring Problem" in $\mathbb{Z}/m\mathbb{Z}$. For any positive integers m and k let $\gamma(k,m)$ denote Waring's number $\pmod m$, the smallest positive integer s such that every integer is a sum of s k-th powers $\pmod m$. It is plain that if m has prime power factorization $m = \Pi_{i=1}^{j} p_i^{e_i}$ then $\gamma(k,m) = \max_i \gamma(k, p_i^{e_i})$ and so we may restrict our attention to prime power moduli.

The case of prime moduli has been thoroughly studied and dates back to Cauchy [9], who proved $\gamma(k,p) \leq k$ for any prime p; see [21] for a further discussion of this case. Estimates for $\gamma(k,p^n)$ date back to the work of Hardy and Littlewood on the classical Waring problem. They established [17, p. 186, Theorem 12] the uniform upper bound $\gamma(k,p^n) \leq 4k$ for any prime power and for odd p the sharper bound

$$\gamma(k,p^n) \leq \frac{p}{p-1}\, k + 1; \tag{2.1}$$

see also Landau [23, Kapitel 1, Satz 31]. This estimate is essentially best possible for arbitrary k. Indeed, if p is odd and $k = p^{e-1}(p-1)$ then every k-th power $\pmod{p^e}$ is either 0 or 1, while if $k = p^{e-1}(p-1)/2$ every k-th power is either $0, 1$ or -1 $\pmod{p^e}$, and so

$$\gamma(p^e - p^{e-1}, p^n) = p^e - 1 \quad \text{and} \quad \gamma(\tfrac{p^e - p^{e-1}}{2}, p^n) = \tfrac{1}{2}(p^e - 1), \tag{2.2}$$

for any $n \geq e$. Similarly, for $p = 2$, as noted in the next paragraph, one has $\gamma(k, 2^n) = 4k$ or $\gamma(k, 2^n) = 4k - 1$ when $k = 2^e$ and $n \geq e + 2$. With the exception of these extremal cases, the upper bound of Hardy and Littlewood can be substantially improved.

For $p = 2$, Subocz [31] determined the exact value of $\gamma(k, 2^n)$. If $k > 1$ is odd then $\gamma(k, 2^n) = 2$ for $n \geq 2$. Suppose k is even, say $k = 2^e k_1$ with $e \geq 1$ and k_1 odd. Then $\gamma(k, 2^n) = 2^n - 1$ if $4 \leq n \leq e+2$, and $\gamma(k, 2^n) = 2^{e+2}$ if $n \geq e+3$ and $k \geq 6$. Small [29],[28] had already treated the cases $k = 2$ and 4: $\gamma(2, 2^2) = 3$, $\gamma(2, 2^n) = 4$ for $n \geq 3$, $\gamma(4, 2^3) = 7$, $\gamma(4, 2^n) = 15$ for $n \geq 4$. Henceforth, we shall assume p is odd.

2.2 $\gamma(k, p^n)$, $\gamma^*(k, p^n)$, and Lemmas.

As noted by Small [29], [28] the main difficulty in going from representations of a number as a sum of k-th powers $\pmod p$ to representations $\pmod{p^n}$ is in dealing with values of k divisible by a power of p that prohibits the lifting of solutions. Small gives a procedure for determining the value of $\gamma(k, p^n)$ and calculates the value for a number of special cases including $k = 2$ and 3. The first case of special interest is the determination of $\gamma(p, p^2)$. Several authors (including the present) independently discovered the bound,

$$\gamma(p, p^2) \leq 4, \tag{2.3}$$

for any prime p; see Corollary 2.2.1. The earliest reference we could find is the work of Bhaskaran [4]. (Small seemed to be unaware of this work and only proved a much weaker bound for $\gamma(p, p^2)$.) The bound is also implicit in the work of Bovey [7], and rediscovered by Benschop [2]. Voloch [34] verified that in fact $\gamma(p, p^2) \leq 3$ for $p \leq 211$ except for $p = 3, 7, 11, 17$ and 59. With a program in UBASIC (see Appendix A) we extended the range to $p \leq 1000$ and found no further exceptions.

For prime power moduli p^n it is convenient to study the related quantity $\gamma^*(k, p^n)$, the smallest s such that every integer is a sum of at most s k-th powers of integers coprime to p, that is, the smallest s such that for any integer a the congruence

$$x_1^k + x_2^k + \cdots + x_s^k \equiv a \pmod{p^n} \tag{2.4}$$

is solvable in integers x_i with $p \nmid x_i$ or $x_i = 0$, $1 \le i \le s$, and $x_1 \neq 0$. The following lemma is well known.

Lemma 2.2.1. *Lifting Lemma. Let $k = p^e k_1$ with $p \nmid k_1$.*

(i) Suppose p is odd. Then for any $n \ge e+1$ we have $\gamma^*(k, p^n) = \gamma^*(k, p^{e+1})$. More specifically, any solution $(x_1, \ldots, x_s)$ of (2.4) with $p \nmid x_i$ for some i and $n = e+1$ can be lifted to a solution $\pmod{p^n}$ for any $n \ge e+1$.

(ii) Suppose $p = 2$. Then for any $n \ge e+2$ we have $\gamma^*(k, 2^n) = \gamma^*(k, 2^{e+2})$, and the analogous lifting statement holds.

Proof. Suppose first that p is odd. The proof is by induction on n starting with $n = e+1$. Let $x_1, \ldots, x_s$ be a solution of (2.4) with $p \nmid x_1$. We lift this to a solution $\pmod{p^{n+1}}$ by finding t such that

$$(x_1 + tp^{n-e})^k + x_2^k + \cdots + x_s^k \equiv a \pmod{p^{n+1}}$$

or equivalently

$$\begin{aligned}(x_1^k + x_2^k + \cdots + x_s^k - \alpha) + (kx_1^{k-1}p^{n-e})t + \\ \binom{k}{2} x_1^{k-2} p^{2(n-e)} t^2 + \cdots + (tp^{n-e})^k \equiv 0 \pmod{p^{n+1}}.\end{aligned} \tag{2.5}$$

That is

$$(x_1^k + \cdots + x_s^k - a) + ktx_1^{k-1}p^{n-e} \equiv 0 \pmod{p^{n+1}}.$$

Here we have used the fact that if $p^i \| j$ then $p^{e-i} \mid \binom{k}{j}$ for $e > i$, and so the remaining terms in the binomial expansion vanish. Dividing by p^n we obtain a linear congruence (mod p) that is solvable for t.

When $p = 2$ extra care needs to be taken since the third term of the binomial expansion $\frac{k(k-1)}{2} t^2 2^{2(n-e)} x_1^{k-2}$ doesn't vanish if $n - e = 1$. Thus we need the stronger assumption that $n \geq e + 2$. □

For odd p, the multiplicative group of units (mod p^n), $G(p^n)$, is cyclic and so we have

Lemma 2.2.2. *For any positive integer k and odd prime power p^n we have*

$$\gamma^*(k, p^n) = \gamma^*(d, p^n)$$

where $d = gcd(k, p^{n-1}(p-1))$. Moreover, if $d \geq n$ then $\gamma(k, p^n) = \gamma(d, p^n)$.

Proof. In short, this follows since the subgroup of k-th powers in $\mathbb{Z}_p^*$ equals the subgroup of d-th powers. To be explicit, let $\gamma^*(k, p^n) = s$, $\gamma^*(d, p^n) = r$, $k = d\omega$ for some $\omega \in \mathbb{N}$. Then for any $a \in \mathbb{Z}$ there exist $x_1, x_2, \cdots, x_s \in G(p^n)$, such that $a \equiv x_1^k + x_2^k + \cdots + x_s^k \pmod{p^n}$, that is $a \equiv (x_1^\omega)^d + (x_s^\omega)^d + \cdots + (x_s^\omega)^d \pmod{p^n}$, which implies that $r \geq s$. On the other hand, $a \equiv y_1^d + y_2^d + \cdots + y_r^d \pmod{p^n}$, for some $y_i \in G(p^n)$. Since $d = gcd(k, \phi(p^n))$ there exist $i, j \in \mathbb{Z}$ so that $d = ik + j\phi(p^n)$ and for any $z \in G(p^n)$ $z^{j\phi(p^n)} \equiv 1 \pmod{p^n}$, hence we have $a \equiv (y_1^i)^k + (y_2^i)^k + \cdots + (y_r^i)^k \pmod{p^n}$, and so $r \leq s$.

The second part of the lemma follows from the observation that if $d \geq n$ and $p|x$ then $x^k \equiv x^d \equiv 0 \pmod{p^n}$. □

Lemma 2.2.3. *For any odd prime power p^n and positive integer k we have*

$$\gamma(k, p^n) \leq \gamma^*(k, p^n) \leq \gamma(k, p^n) + 1.$$

Proof. We may assume by Lemma 2.2.2 that $k|p^{n-1}(p-1)$, say $k = p^e k_1$ with $0 \leq e \leq n-1$ and $k_1|(p-1)$. From the lifting lemma, Lemma 1.1, we have $\gamma^*(k, p^n) = \gamma^*(k, p^{e+1})$, and so we may assume further that $e = n - 1$, that is

$$k = p^{n-1} k_1 \qquad \text{with } k_1|(p-1).$$

In this case $k \geq p^{n-1} \geq n$ and so $p|x_i$ implies that $p^n|x_i^k$, that is $x_i^k \equiv 0 \pmod{p^n}$. It follows that $\gamma^*(k, p^n) = \gamma(k, p^n)$ unless 0 has no nontrivial representation as a sum of less than or equal to $\gamma^*(k, p^n)$ k-th powers. In the latter case we represent -1 in a nontrivial manner and add 1, thus we have the inequality above. □

Next, we obtain Landau's result in (2.1).

Theorem 2.2.1. *Let $k = p^e k_1$ with $p \nmid k_1$. Suppose p is odd, we have*

$$\gamma(k, p^n) \leq \left(\frac{p}{p-1}\right) k + 1$$

Proof. We start by finding an upper bound for $\gamma^*(k, p^{e+1})$. Let $a \in \mathbb{Z}/(p^{e+1})$, then a can be uniquely represented in the form

$$a \equiv u_0 + u_1 p + u_2 p^2 + \cdots + u_e p^n \pmod{p^{e+1}}, \tag{2.6}$$

where $u_i \in \mathbb{Z}/(p) = \{0, 1, 2, \ldots, p-1\}$ for $0 \leq i \leq e$.

We assume as in the proof of Lemma 2.2.3 that $k_1|(p-1)$. Since u_i can be expressed as a sum of $\gamma_1 = \gamma(k, p)$ k-th powers for all i and by Cauchy bound

$$\gamma_1 = \gamma(k, p) = \gamma((k, p-1), p) \leq (k, p-1) = k_1$$

we have

$$\begin{aligned} \gamma^*(k, p^{e+1}) &\leq \gamma_1(1 + p + p^2 + \cdots + p^e) \\ &\leq k_1 p^e \left(1 + \frac{1}{p} + \cdots + \frac{1}{p^e}\right) \\ &\leq k \left(\frac{p}{p-1}\right). \end{aligned}$$

Finally by the lifting lemma, Lemma 2.2.1, and Lemma 2.2.3 we have the desired inequality.

□

The following lemma sharpens a result of Bovey [7, Theorem 1].

Lemma 2.2.4. *Let p be a prime and k be a positive integer with $k = p^e k_1$, where $p \nmid k_1$. Put $\gamma_n = \gamma(k, p^n)$. In particular $\gamma_1 = \gamma(k_1, p)$. Then*

(i) For any positive integer n, $\gamma_{n+1} \leq (2\gamma_1 + 1)\gamma_n + \gamma_1$.

(ii) For any positive integer n,

$$\gamma(k, p^n) \leq \frac{1}{2}[(2\gamma_1 + 1)^n - 1].$$

Proof. Let $k = p^e k_1$ with $p \nmid k_1$ and $\gamma_1 = \gamma(k, p) = \gamma(k_1, p)$ the latter equality following from $x^p \equiv x \pmod{p}$ for all x. Put $s = \gamma_n = \gamma(k, p^n)$. If $\gamma_{n+1} = s$ the inequality in part (i) is immediate. Otherwise, some integer is not a sum of s k-th powers $\pmod{p^{n+1}}$. Letting m denote the smallest such non-negative integer, we have $m - 1$ is a sum of s k-th powers $\pmod{p^{n+1}}$, and so $m = (m-1) + 1$ is a sum of $s + 1$ k-th powers $\pmod{p^{n+1}}$. Thus the set of all sums of $s + 1$ k-th powers $\pmod{p^{n+1}}$ has larger cardinality than the set of all sums of s k-th powers, and so there exist integers $y_1, \ldots, y_{s+1}$ such that $y_1^k + \cdots + y_{s+1}^k$ is not congruent to any number of the form $-x_1^k - x_2^k - \cdots - x_s^k \pmod{p^{n+1}}$. On the other hand, since every value $\pmod{p^{n+1}}$ is of the form $u + p^n v$ where u runs through a complete residue system $\bmod p^n$ and v a complete residue system $\pmod{p}$ we know there exist integers $x_1, \ldots, x_s$ and v_0 such that

$$-(x_1^k + x_2^k + \cdots + x_s^k) + p^n v_0 \equiv y_1^k + \cdots + y_{s+1}^k \pmod{p^{n+1}}.$$

Moreover, by our assumption on the y_i we have $p \nmid v_0$. We see that $p^n v_0$ is a sum of $(2s+1)$ k-th powers. Since every integer $\bmod p^{n+1}$ is of the form $u + p^n v_0 v$ where u is taken $\pmod{p^n}$ and $v \pmod{p}$ we conclude that

$$\gamma_{n+1} \leq s + (2s+1)\gamma_1 = s(2\gamma_1 + 1) + \gamma_1 = \gamma_n(2\gamma_1 + 1) + \gamma_1. \tag{2.7}$$

The inequality in part (ii) follows easily by induction on n. The case $n = 1$ is trivial. Assuming the result for n we have

$$\gamma_{n+1} \leq \gamma_n(2\gamma_1 + 1) + \gamma_1 \leq \frac{1}{2}[(2\gamma_1 + 1)^n - 1](2\gamma_1 + 1) + \gamma_1 = \frac{1}{2}[(2\gamma_1 + 1)^{n+1} - 1].$$

□

Corollary 2.2.1. *If p is an odd prime, $k = p^e k_1$ with $p \nmid k_1$ and $\gamma_1 = \gamma(k_1, p)$ then for any positive integer n,*

$$\gamma(k, p^n) \leq \begin{cases} \frac{1}{2}[(2\gamma_1 + 1)^{\min(e+1,n)} - 1] & \text{if } k \text{ is odd,} \\ \\ \frac{1}{2}[(2\gamma_1 + 1)^{\min(e+1,n)} + 1] & \text{if } k \text{ is even.} \end{cases}$$

Proof. If $n \leq e + 1$ the result follows immediately from Lemma 2.2.4 (ii). If $n > e + 1$ and $a \in \mathbb{Z}$, we start by obtaining a representation of a as a sum of $s \leq \frac{1}{2}[(2\gamma_1 + 1)^{e+1} - 1]$ nonzero k-th powers $\pmod{p^{e+1}}$. If k is odd then 0 has a primitive representation as a sum of k-th powers, so the result in follows from the Lemma 2.2.3 and the lifting lemma, Lemma 2.2.1. □

In comparison, Bovey [7] proved $\gamma(k, p^n) \leq \frac{1}{2}(3\gamma_1)^{\min(e+1,n)}$. If $e = 1$ and $(k_1, p - 1) = 1$ so that $\gamma_1 = 1$ then we get from Corollary 2.2.1, $\gamma(pk_1, p^n) \leq 4$. If $e = 1$ and $p > k_1^4$ so that $\gamma_1 \leq 2$ (see eg. [21]) then we have $\gamma(k, p^n) \leq 12$. Voloch [34, Lemma 3] obtained the sharper bound $\gamma(k, p^n) \leq 8$ under the constraint $e = 1$, $p \geq \max\{27k_1^6, 13\}$.

2.3 Old and new Results.

S. Chowla, Mann and Strauss [25], showed that for prime moduli we have the uniform bound

$$\gamma(k, p) \leq [k/2] + 1,$$

provided that k is not divisible by $\frac{p-1}{2}$ when p is odd. Our first theorem generalizes this to prime powers.

Theorem 2.3.1. *For any k and odd prime power p^n with k not divisible by $\frac{p-1}{2}$, we have*

$$\gamma(k, p^n) \leq [(k, \phi(p^n))/2] + 2 \leq [k/2] + 2.$$

For prime powers the extra 1 in the upper bound is sometimes needed. For example if $p \equiv 3 \pmod 4$ then $\gamma(2, p^2) = 3$ since p cannot be represented as a sum of two squares (mod p^2). Indeed, $x^2 + y^2 \equiv 0 \pmod p$ implies $x \equiv y \equiv 0 \pmod p$ since $\left(\frac{-1}{p}\right) = -1$, and so $x^2 + y^2 \equiv 0 \pmod{p^2}$

Proof. As noted before, the slightly stronger inequality

$$\gamma(k, p^n) \leq k/2 + 1 \tag{2.8}$$

was established by S. Chowla, Mann and Straus [25] when $n = 1$ and so we assume that $n \geq 2$. First we treat the case $k = p^{n-1}k_1$ with $k_1|(p-1)$, $k_1 \leq (p-1)/3$, and prove that 2.8 holds. In particular $p \geq 5$. If $k_1 = 1$ then by Lemma 2.2.4 (ii),

$$\gamma(k, p^n) \leq \frac{1}{2}(3^n - 1) \leq \frac{1}{2}p^{n-1} + 1 = \frac{k}{2} + 1$$

unless $p = 5$, $n = 2$. A computer search shows $\gamma^*(5, 5^2) = 3$, so the inequality is still valid. If $k_1 = 2$ then $p \geq 7$ and $\gamma_1 := \gamma(2, p) = 2$. Thus by Lemma 2.2.4 (ii), $\gamma(k, p^n) \leq \frac{1}{2}(5^n - 1) \leq p^{n-1} + 1 = \frac{k}{2} + 1$ unless $(p, n) = (7, 2), (7, 3)$ or $(11, 2)$. One checks on a computer that $\gamma^*(14, 49) = 7$, $\gamma^*(22, 121) = 6$ and then by the recursion Lemma 2.2.4 (i) and since $\gamma(98, 7^2) \leq \gamma^*(98, 7^2) = \gamma^*(14, 7^2) = 7$,

$$\gamma(98, 7^3) \leq [2\gamma(98, 7) + 1]\gamma(98, 7^2) + \gamma(98, 7) \leq 7 \cdot 5 + 2 = 37,$$

and so again the result holds.

Next we prove that for $k_1 \geq 3$ and $n \geq 2$ we have $\gamma(k_1 p^{n-1}, p^n) \leq k/2$. Since $p - 1 \geq 3k_1 \geq 9$ and $k_1|(p-1)$ we have $p \geq 13$; there is no such k_1 when $p = 11$. Now by Lemma 2.2.4 (ii) and the fact that $\gamma_1 = \gamma(k_1, p) \leq k_1/2 + 1$ we have

$$\gamma(k, p^n) \leq \frac{1}{2}\left[(2(k_1/2 + 1) + 1)^n - 1\right] \leq \frac{1}{2}(k_1 + 3)^n.$$

If $k_1 = 3$ we get $\gamma(k, p^n) \le \frac{1}{2}6^n \le \frac{3}{2}p^{n-1} = k/2$, since $p \ge 13$. Suppose $k_1 \ge 4$ so that $\frac{7}{13}(k_1+3) \le k_1$. Now $k_1 \le \frac{p-1}{3}$ implies that $\frac{k_1+3}{p} \le \frac{7}{13}$ and so

$$\gamma(k, p^n) \le \frac{1}{2}(k_1+3)(k_1+3)^{n-1} \le \frac{1}{2}(k_1+3)(\frac{7}{13})^{n-1}p^{n-1} \le \frac{1}{2}(\frac{7}{13})^{n-2}k.$$

Finally, let $k = k_1 p^e$, be an arbitrary value with $gcd(p, k_1) = 1$, $\frac{p-1}{2} \nmid k_1$ and put $k_1' = (k_1, p-1)$, $e' = \min(e, n-1)$. Then for any $n \ge 1$ we have by Lemma 2.2.2

$$\gamma(k, p^n) = \gamma(k_1 p^e, p^n) \le \gamma^*(k_1 p^e, p^n) = \gamma^*(k_1' p^{e'}, p^n).$$

By Lemmas 2.2.1 and 2.2.3 and inequality 2.8 we then have

$$\gamma(k, p^n) \le \gamma^*(k_1' p^{e'}, p^{e'+1}) \le \gamma(k_1' p^{e'}, p^{e'+1}) + 1 \le \frac{1}{2}k' + 2,$$

where $k' = k_1' p^{e'} = (k, \phi(p^n))$. □

I. Chowla [10] showed that if p is odd and $\frac{p-1}{2}$ is not a divisor of k then $\gamma(k, p^n) \ll k^{.88}$. Dodson [15] sharpened this to $\gamma(k, p^n) \ll k^{7/8}$. Finally, Bovey [7] established

$$\gamma(k, p^n) \ll_\epsilon k^{\frac{1}{2}+\epsilon}, \tag{2.9}$$

for odd p with $\frac{p-1}{2}$ not dividing k. Here we eliminate the ϵ.

Theorem 2.3.2. *For any k, n, p with $(p-1)/2$ not dividing k we have*

$$\gamma(k, p^n) \ll \sqrt{k}.$$

We also establish a more general result. Let $t = (p-1)/(p-1, k)$ and $\phi(t)$ be the Euler-phi function.

Theorem 2.3.3. *For any $\epsilon > 0$ there is a constant $c(\epsilon)$ such that if $\phi(t) \ge \frac{1}{\epsilon}$ then*

$$\gamma(k, p^n) \le c(\epsilon)k^\epsilon.$$

Notice that, Theorem 2.3.2 is obtained on taking $\epsilon = 1/2$.

Cipra, Cochrane and Pinner [21] proved Theorems 2.3.2 and 2.3.3 for the case of prime moduli. Konyagin [22] was the first to obtain $\gamma(k,p) \ll_\epsilon k^\epsilon$ for $t > c(\epsilon)$. This result and Theorem 2.3.2 were conjectured by Heilbronn [18] for the case of prime moduli. Heilbronn [18, Theorem 8] proved $\gamma(k,p) \ll_t p^{1/\phi(t)}$.

Here, we will establish an even more general result which will give us Theorems 2.3.2 and 2.3.3.

Theorem 2.3.4. *Let q be a positive integer and put $t = (p-1)/(p-1,k)$. If $\phi(t) \geq q$ then $\gamma(k,p^n) \leq C(q)\ k^{1/q}$, for some constant $C(q)$.*

Theorem 2.3.2 is just the case $q = 2$, while Theorem 2.3.3 follows by taking $q > 1/\epsilon$.

To prove the theorem we start by generalizing two lemmas of Bovey [8, Lemma 3, Lemma 5]. For any n-tuple $u = (u_1, \dots, u_n) \in \mathbb{R}^n$ let $\|u\|_1 = \sum_{i=1}^n |u_i|$.

Lemma 2.3.1. *Let $a_1, a_2, \dots, a_n, m$ be integers with $m > 0$, and $gcd(a_1, a_2, \dots, a_n, m) = 1$, and let $T : \mathbb{Z}^n \to \mathbb{Z}$ be the linear function given by $T(u) = \sum_{i=1}^n a_i u_i$. Suppose that $v_1, \dots, v_n \in \mathbb{Z}^n$ are linearly independent vectors with $T(v_i) \equiv 0 \pmod m$, $1 \leq i \leq n$. Then for any integer a there exists a vector $u \in \mathbb{Z}^n$ with $T(u) \equiv a \pmod m$ and $\|u\|_1 \leq \frac{1}{2}\sum_{i=1}^n \|v_i\|_1$.*

Proof. Since $\gcd(a_1, \dots, a_n, m) = 1$ there exists $w \in \mathbb{Z}^n$ with $T(w) \equiv a \pmod m$. Say $w = \sum_{i=1}^n x_i v_i$ for some $x_i \in \mathbb{R}$, $1 \leq i \leq n$. Now $x_i = y_i + \epsilon_i$ for some $y_i \in \mathbb{Z}$ and $\epsilon_i \in \mathbb{R}$ with $|\epsilon_i| \leq 1/2$, $1 \leq i \leq n$. Put $u = \sum_{i=1}^n \epsilon_i v_i = w - \sum_{i=1}^n y_i v_i$. Then $T(u) \equiv a \pmod m$ and $\|u\|_1 \leq \frac{1}{2}\sum_{i=1}^n \|v_i\|_1$. □

The next lemma generalizes Heilbronn's inequality [18, Theorem 8] from p to p^n,

Lemma 2.3.2. *For any positive integer t there is a constant $c_1(t)$ such that if $k = k_1 p^{n-1}$ with $k_1 | (p-1)$ and $(p-1)/k_1 = t$, then*

$$\gamma(k, p^n) \leq c_1(t) p^{n/\phi(t)}.$$

Proof. We start by proving the same upper bound for the "easy" Waring's number $\delta(k, p^n)$ defined to be the minimal s such that every integer is a plus-minus sum of at most s k-th powers $\pmod{p^n}$, that is

$$\pm x_1^k \pm x_2^k \pm \cdots \pm x_s^k \equiv a \pmod{p^n}$$

is solvable for all a. Let $t = (p-1)/k_1$ and put $r = \phi(t)$. Let R be a primitive t-th root of one $\pmod{p^n}$, $\Phi_t(x)$ be the t-th cyclotomic polynomial over $\mathbb{Q}$ of degree r and ω be a primitive t-th root of unity over $\mathbb{Q}$. We claim that $\Phi_t(R) \equiv 0 \pmod{p^n}$. Say $x^t - 1 = \prod_{d|t} \Phi_d(x)$. Then $\prod_{d|t} \Phi_d(R) \equiv 0 \pmod{p^n}$. If $\Phi_d(R) \equiv 0 \pmod{p}$ for some $d \mid t$ then $ord_p(R) \leq t$. Since $ord_p(R) = t$ we know that $\Phi_d(R) \equiv 0 \pmod{p}$ if and only if $d = t$. Thus $\Phi_t(R) \equiv 0 \pmod{p^n}$. The set of k-th power units $\pmod{p^n}$ is just $\{1, R, R^2, \ldots, R^{t-1}\}$. Let $f : \mathbb{Z}^r \to \mathbb{Z}[\omega]$ be given by

$$f(x_1, x_2, \ldots, x_r) = x_1 + x_2\omega + \cdots + x_r\omega^{r-1}.$$

Then f is a one-to-one $\mathbb{Z}$-module homomorphism.

Consider the linear congruence

$$x_1 + Rx_2 + R^2x_3 + \cdots + R^{r-1}x_r \equiv 0 \pmod{p^n}. \tag{2.10}$$

By the box principle, we know there is a nonzero solution of the congruence (2.10) in integers $v_1 = (a_1, a_2, \ldots, a_r)$ with $|a_i| \leq p^{n/r}$, $1 \leq i \leq r$. For $2 \leq i \leq r-1$ set $v_i = f^{-1}(\omega^{i-1} f(v_1))$. Then $v_1, \ldots, v_r$ form a set of linearly independent solutions of (2.10) and so by Lemma 2.3.1 for any $a \in \mathbb{Z}$ there is an r-tuple of integers $u = (u_1, \ldots, u_r)$ such that

$$u_1 + u_2R + u_3R^2 + \cdots + u_rR^{r-1} \equiv a \pmod{p^n},$$

and $\sum_{i=1}^{r} |u_i| \le \frac{1}{2}\sum_{i=1}^{r} \|v_i\|_1$. Thus $\delta(k,p^n) \le \frac{1}{2}\sum_{i=1}^{r} \|v_i\|_1$. Now plainly $\|v_i\|_1 \ll_t p^{n/r}$. Indeed, as shown in [8], $\|v_i\|_1 \le r(A(t)+1)^r p^{n/r}$, where $A(t)$ is the maximal absolute value of the coefficients of $\Phi_t(x)$. Thus $\delta(k,p^n) \ll_t p^{n/r}$. Now $\gamma(k,p^n) \le (t-1)\delta(k,p^n)$ since $-1 \equiv R + R^2 + \cdots + R^{t-1} \pmod{p^n}$, and so the lemma follows. □

Proof of Theorem 2.3.4. We may assume $k = k_1 p^{n-1}$, with $k_1 | (p-1)$. The theorem was established in the case $n = 1$ in [21, Theorem 1]; say

$$\gamma(k,p) \le c_q \, k^{1/q}, \tag{2.11}$$

for some constant c_q, whenever $\phi(t) \ge q$. In [14] the value of $c_2 = 83$ is obtained.

Suppose first that $p > 3^q c_q^q k_1$. Put $\gamma_1 = \gamma(k_1, p)$. Then by Lemma 2.2.4 (ii) and (2.11) we have

$$\begin{aligned} \gamma(k,p^n) \le \frac{1}{2}((2\gamma_1+1)^n - 1) &\le (3\gamma_1)^n \\ &\le 3^n c_q^n k_1^{n/q} \\ &= 3^n c_q^n k_1^{1/q} k_1^{\frac{n-1}{q}}, \end{aligned}$$

and it follows from $k_1 < p/(3^q c_q^q)$ that

$$\begin{aligned} \gamma(k,p^n) &\le 3^n c_q^n k_1^{1/q} \left(\frac{p}{3^q c_q^q}\right)^{\frac{n-1}{q}} \\ &= 3c_q (p^{n-1}k_1)^{1/q} \\ &= 3c_q k^{1/q}. \end{aligned}$$

Suppose next that $p \le 3^q c_q^q k_1$, so that $t = \dfrac{p-1}{k_1} \le 3^q c_q^q$. Put

$$c^*(q) = \max_{t \le 3^q c_q^q} c_1(t),$$

where $c_1(t)$ is as given in Lemma 2.3.2. Then by Lemma 2.3.2 and the assumption $r = \phi(t) \ge q$, we have

$$\begin{aligned} \gamma(k,p^n) &\le c_1(t) p^{n/\phi(t)} \\ &\le c^*(q) p^{n/q} \\ &= c^*(q) p^{\frac{n-1}{q}} p^{1/q}. \end{aligned}$$

Therefore, from $p \leq 3^q c_q^q k_1$,

$$\begin{aligned} \gamma(k, p^n) &\leq c^*(q) p^{\frac{n-1}{q}} 3 c_q k_1^{1/q} \\ &= 3 c^*(q) c_q k^{1/q}. \end{aligned}$$

□

Chapter 3

Waring's Problem over Number Fields.

In this chapter we will generalize some of the theorems and lemmas of Chapter 2, as well as some of the other results found in the literature. The methods used in this chapter were motivated by the work of R. Stemmler [30], but improvements will be made.

Unless otherwise specified, from this point on we let F be any algebraic number field, R it's ring of integers, and for a fixed positive integer k we let R_k be the subring of R generated by the k-th powers of elements of R. Furthermore, let $\mathcal{P}$ be a prime ideal of R, such that $\mathcal{P}$ lies over the rational prime p. Suppose that $\mathcal{P}$ has ramification index e and degree of inertia f and set $q = p^f$. Assume that $k = p^r k_1$ with $gcd(k_1, p) = 1$ and $\mathcal{P}^n \| k$, so that $n = er$.

3.1 R_k, $\gamma_R(k)$ and $\delta_R(k)$.

Some work has been done on the relationship between R and R_k. Paul Bateman and Rosemarie Stemmler in [1] gave a detailed characterization of R_k when k is a rational prime. Later M. Bhaskaran generalized that result to any positive integer k in [3] as follows:

Theorem 3.1.1. *[3, Bhaskaran, Theorem 1.] $R = R_k$ if and only if*

(I) k is relatively prime to the discriminant of F,

(II) k has no factor of the form $(p^f - 1)/(p^d - 1)$, where p is a rational prime which has

a prime ideal factor in R of degree of inertia f, and d is a divisor of f such that $f/d > 1$.

Notice that conditions (I) and (II) above are equivalent to the following conditions (i) and (ii) respectively

(i) None of the prime divisors of k ramify.

(ii) If $\mathcal{P}$ is a prime ideal of R such that $\mathcal{P}|k$, then every element in the finite field $R/\mathcal{P}$ is expressible as a sum of k-th powers.

Let $\gamma_R(k)$ be the least positive integer s, such that the equation

$$x_1^k + x_2^k + \cdots + x_s^k = \alpha, \tag{3.1}$$

is solvable for all totally positive $\alpha \in R_k$, with $x_i \in R$ for $i = 1, 2, \ldots, s$, and let $\delta_R(k)$ be the least positive integer s, such that the equation

$$\pm x_1^k \pm x_2^k \pm \cdots \pm x_s^k = \alpha, \tag{3.2}$$

is solvable for all $\alpha \in R_k$, with $x_i \in R$ for $i = 1, 2, \ldots, s$. Note that, when k is odd $\delta_R(k)$ and $\gamma_R(k)$ are equal since $(-1)^k = -1$. In general if -1 can be expressed as a sum of k-th powers and ρ is the minimal positive integer s such that -1 can be expressed in at most s k-th powers, then

$$\gamma_R(k) \leq \rho\delta_R(k).$$

Also we note that in the proof of Theorem 3.1.1 listed above, Bhaskaran showed that when $R = R_k$, $\delta_R(k)$ is bounded above by a constant depending only on k, but he did not produce an explicit bound.

For any ideal $\mathfrak{M}$ in R, let ${}_{\mathfrak{M}}A_k$ be the set of elements in R which are expressible as a sum of k-th powers $\pmod{\mathfrak{M}}$. In Lemma 3.1.1 we show that ${}_{\mathfrak{M}}A_k$ is a subring of R. We define (as in [30]) $\delta(k, \mathfrak{M})$ to be the least positive integer s, such that every element in ${}_{\mathfrak{M}}A_k$ is congruent to an element of the type $\pm x_1^k \pm x_2^k \pm \cdots \pm x_s^k \pmod{\mathfrak{M}}$, with $x_i \in R$ for $i = 1, 2, \ldots, s$. We also define $\gamma(k, \mathfrak{M})$ to be the least positive integer s such that every

element of ${}_{\mathfrak{M}}A_k$ is congruent to an element of the the type $x_1^k + x_2^k + \cdots + x_s^k \pmod{\mathfrak{M}}$. Note that, when k is odd $\gamma(k, \mathfrak{M}) = \delta(k, \mathfrak{M})$ since $(-1)^k = -1$.

Lemma 3.1.1. *${}_{\mathfrak{M}}A_k$ is a subring of R.*

Proof. Let $\mathcal{S}$ be the set of sums of k-th powers in $R/\mathfrak{M}$. Note that $\mathcal{S}$ is a subring of $R/\mathfrak{M}$ since it is closed under addition and multiplication. Also, $-1 \in \mathcal{S}$ since $-1 \equiv |R/\mathfrak{M}| - 1 \pmod{\mathfrak{M}}$, where $|R/\mathfrak{M}|$ is the order of the finite additive group $R/\mathfrak{M}$. The set ${}_{\mathfrak{M}}A_k$ is the inverse image of the subring $\mathcal{S}$ under the canonical map $R \longrightarrow R/\mathfrak{M}$.

□

There are two results that we can apply at this point to reduce the global problem of finding upper bounds for $\gamma_R(k)$ and $\delta_R(k)$ to the local problem of finding upper bounds for $\gamma(k, \mathfrak{M})$ and $\delta(k, \mathfrak{M})$. One result is due to B. J. Birch [5] which was mentioned in the Introduction.

The second result due to R. Stemmler makes use of the identity for the $(k-1)$-th difference of x^k (also used by R. Stemmler and P. Bateman in [1])

$$\sum_{i=0}^{k-1}(-1)^{k-1-i}\binom{k-1}{i}(x+i)^k = (k!)x + \frac{1}{2}(k-1)k!.$$

Notice that this equation implies that

$$(k!)R \subseteq R_k \subseteq R.$$

Hence R_k consists of certain residue classes in $R/(k!)R$.

Consequently, if $\delta(k, (k!)) = s$, $\alpha \in R_k$, and

$$\alpha - \frac{1}{2}(k-1)k! = \pm x_1^k \pm x_2^k \pm \cdots \pm x_s^k + (k!)C, \text{ for some } C \in R,$$

then

$$\alpha = \pm x_1^k \pm x_2^k \pm \cdots \pm x_s^k + (k!)C + \frac{1}{2}(k-1)k!,$$

that is

$$\alpha = \pm x_1^k \pm x_2^k \pm \cdots \pm x_s^k + \sum_{i=0}^{k-1} (-1)^{k-1-i} \binom{k-1}{i} (C+i)^k.$$

Thus we have

$$\delta_R(k) \leq \delta(k,(k!)) + \sum_{i=0}^{k-1} \binom{k-1}{i},$$

and since $\sum_{i=0}^{k-1} \binom{k-1}{i} = 2^{k-1}$, we have the following key inequality,

$$\delta_R(k) \leq \delta(k,(k!)) + 2^{k-1}. \tag{3.3}$$

In particular, $\delta_R(k)$ is finite, and we also have

$$\gamma_R(k) \leq \rho(\delta(k,(k!)) + 2^{k-1}), \tag{3.4}$$

provided that -1 can be expressed as a sum of at most ρ k-th powers.

Since R is a Dedekind Domain, the ideal $(k!)$ in R has a unique prime ideal factorization, say $(k!) = \mathcal{P}_1^{r_1}\mathcal{P}_2^{r_2}\cdots\mathcal{P}_t^{r_t}$. Furthermore, from the Chinese Remainder Theorem it is plain that

$$\gamma(k,(k!)) = \max_{1\leq i\leq t} \gamma(k,\mathcal{P}_i^{r_i}),$$

Let d be the degree of the number field extension. Stemmler obtained that

$$\delta(k,(k!)) \leq \begin{cases} d(2k-1)+1 & \text{when } k \text{ is odd,} \\ d(4k-1)+1 & \text{when } k \text{ is even.} \end{cases}$$

Stemmler's results depend on the degree of the extension except for the case when k is a prime. For an odd prime exponent $p \geq 3$ Stemmler obtained

$$\gamma_R(p,p!) = \delta_R(p,p!) \leq (p+2)/3.$$

For the case when $p = 2$ Stemmler obtained the global result

$$\delta_R(2) \leq 3.$$

We will now focus our attention on finding an upper bound for $\delta(k, \mathcal{Q}^m)$ and $\gamma(k, \mathcal{Q}^m)$, where $\mathcal{Q}$ is a prime ideal of R, and $m \geq 1$ with $\mathcal{Q}^m \| (k!)$. That is, we can consider congruences of the form

$$\pm x_1^k \pm x_2^k \pm \cdots \pm x_s^k \equiv \alpha \pmod{\mathcal{Q}^m}, \tag{3.5}$$

for any $\alpha \in R_k$, or equivalently we can consider the equation

$$\pm \overline{x}_1^k \pm \overline{x}_2^k \pm \cdots \pm \overline{x}_s^k = \overline{\alpha}, \tag{3.6}$$

over $R/\mathcal{Q}^m$.

We can also consider the localization of R at the prime ideal $\mathcal{Q}$.

Lemma 3.1.2. *Let R be any Dedekind domain, and $\mathcal{Q}$ a prime ideal of R. Then $R/\mathcal{Q}^m$ and $R_{\mathcal{Q}}/\mathcal{Q}_{\mathcal{Q}}^m$ are isomorphic, where $R_{\mathcal{Q}}$ is the localization of R at $\mathcal{Q}$, and $\mathcal{Q}_{\mathcal{Q}}$ is it's unique maximal ideal.*

Proof. Consider the map $\Psi : R \longrightarrow R_{\mathcal{Q}}/{\mathcal{Q}_{\mathcal{Q}}}^m$, given by $\Psi(a) = a + {\mathcal{Q}_{\mathcal{Q}}}^m$. Ψ is a ring homomorphism, and for any $a \in R$ we have $a \in ker(\Psi)$ if and only if $a \in {\mathcal{Q}_{\mathcal{Q}}}^m \cap R = \mathcal{Q}^m$, hence Ψ induces an injective homomorphism $\overline{\Psi} : R/\mathcal{Q}^m \longrightarrow R_{\mathcal{P}}/{\mathcal{Q}_{\mathcal{Q}}}^m$, given by $\overline{\Psi}(a + \mathcal{Q}^m) = \Psi(a) = a + {\mathcal{Q}_{\mathcal{Q}}}^m$.

To show the surjection, recall that since R is a Dedekind domain then so is $R_{\mathcal{Q}}$, so if $\mathcal{A}$ and $\mathcal{B}$ are two ideal in R with $\mathcal{A} = \mathcal{P}_1^{e_1}\mathcal{P}_2^{e_2}\cdots\mathcal{P}_l^{e_l}$ and $B = \mathcal{Q}_1^{f_1}\mathcal{Q}_2^{f_2}\cdots\mathcal{Q}_m^{f_m}$, such that $\mathcal{Q}_i \neq \mathcal{P}_j$ for all i, j, then $\mathcal{A} + \mathcal{B} = R$ since no maximal ideal can contain $\mathcal{A} + \mathcal{B}$.

Pick a nonzero element $(a/b) + {\mathcal{Q}_{\mathcal{Q}}}^m \in R_{\mathcal{Q}}/{\mathcal{Q}_{\mathcal{Q}}}^m$ (that is a, b in R and b is not in $\mathcal{Q}$). We wish to find $x + \mathcal{Q}^m \in R/\mathcal{Q}^m$ such that $\overline{\Psi}(x + \mathcal{Q}^m) = \dfrac{a}{b} + \mathcal{Q}_{\mathcal{Q}}^m$. Equivalently, we need to find $x + \mathcal{Q}^m \in R/\mathcal{Q}^m$ such that $bx - a \in \mathcal{Q}_{\mathcal{Q}}^m$. Since b is not in $\mathcal{Q}$ then $(b)R$ is not contained in $\mathcal{Q}$, so $(b)R + \mathcal{Q}^m = R$. Hence there exists $\beta \in R$ and $\alpha \in \mathcal{Q}^m$, with $\beta b + \alpha = 1$, and so $\beta b - 1 = -\alpha \in \mathcal{Q}^m$. Therefore, we have

$$\frac{a}{b}(\beta b - 1) = a\beta - \frac{a}{b} = \frac{-\alpha a}{b} \in \mathcal{Q}^m,$$

which implies that

$$a\beta \equiv \frac{a}{b} \pmod{\mathcal{Q}_{\mathcal{Q}}^m}.$$

So take $x \equiv a\beta \pmod{\mathcal{Q}^m}$. Thus $\overline{\Psi}$ is an isomorphism.

One could also prove the surjection for rings of integers by noting that

$$|R/\mathcal{Q}^m| = |R/\mathcal{Q}|^m = |R_{\mathcal{Q}}/\mathcal{Q}_{\mathcal{Q}}|^m = \left|R_{\mathcal{Q}}/\mathcal{Q}_{\mathcal{Q}}^m\right|.$$

□

Thus we can consider (3.6) over the ring $R_{\mathcal{Q}}/\mathcal{Q}_{\mathcal{Q}}^m$ instead of $R/\mathcal{Q}^m$.

3.2 Lifting Theorems.

In this section we will prove a modified version of a The Hensel lifting lemma used by Stemmler, [30, Theorem 5]. It yields an analog to the lifting lemma, Lemma 2.2.1, from Chapter 2.

Definition 3.2.1. *Let R be the ring of integers in a number field and $\mathcal{P}^m$ be a prime ideal power in R. Let $R_{\mathcal{P}}$ be the localization of R at $\mathcal{P}$ and let $\pi \in R_{\mathcal{P}}$ be a uniformizer. A solution $x_1, x_2, \cdots, x_s$ to the congruence*

$$\pm x_1^k \pm x_2^k \pm \cdots \pm x_s^k \equiv a \pmod{\pi^m}$$

is called primitive *if and only if $gcd(x_1, x_2, \cdots, x_s, \pi) = 1$ in $R_{\mathcal{P}}$.*

First we have the following lemma,

Lemma 3.2.1. *Let R be a ring of integers and $\mathcal{P}$ a prime ideal in R lying over the rational prime p with ramification index e. Let $R_{\mathcal{P}}$ be the localization of R at $\mathcal{P}$, and let π be the*

uniformizer. Suppose k and j are integers such that $p^r \| k$, with $r \geq 0$ and $k \geq j \geq 2$. Then for any x and t the binomial term $\binom{k}{j} x^{k-j} \pi^{j(n-er)} t^j$ is divisible by π^{n+1} where

$$n \geq \begin{cases} er + \left\lceil \frac{e+1}{p-1} \right\rceil & \text{if } r > 0, \\ 1 & \text{when } r = 0. \end{cases}$$

Proof. For any $X \in \mathbb{Z}$ define $\nu_p(X)$ to be the the multiplicity of p dividing X, and for any $Y \in R_{\mathcal{P}}$ define $\nu_\pi(Y)$ to be the the multiplicity of π dividing Y. Let $k = p^r k_1$ and $j = p^i j_1$ with $r \geq 1$ and $i \geq 0$ where $p \nmid k_1, j_1$. Then

$$\binom{k}{j} = \frac{k}{j}\binom{k-1}{j-1} = p^{r-i}\frac{k_1}{j_1}\binom{k-1}{j-1}.$$

That is,

$$p^{r-i} \Big| \binom{k}{j}.$$

Thus,

$$\nu_p\left[\binom{k}{j}\right] \geq \max\{r-i, 0\} \text{ for any } r \text{ and } i.$$

Now, since $\pi^e \| p$ we have that $\binom{k}{j} x^{k-j} \pi^{j(n-er)} t^j$ is divisible by $\pi^{e \max\{r-i,0\}+j(n-er)}$, that is,

$$\nu_\pi\left[\binom{k}{j} x^{k-j} \pi^{j(n-er)} t^j\right] \geq e\max\{r-i, 0\} + j(n-er).$$

So when $i \geq r \geq 1$

$$\nu_\pi\left[\binom{k}{j} x^{k-j} \pi^{j(n-er)} t^j\right] \geq j(n-er) \geq (n-er)p^i \geq (n-er)p^r.$$

In this case the binomial term $\left(x^{k-j}\pi^{j(n-er)}t^j\right)$ is divisible by π^{n+1} if $n+1 \leq (n-er)p^r$, or equivalently

$$n \geq er + \frac{er+1}{p^r - 1}.$$

Since

$$\frac{er+1}{e+1} = r - \frac{r-1}{e+1} \leq r \leq \frac{p^r-1}{p-1},$$

we have

$$\frac{er+1}{p^r-1} \leq \frac{e+1}{p-1}.$$

Thus the lemma is true when

$$n \geq er + \frac{e+1}{p-1}.$$

If $i = 0$ then

$$\nu_\pi \left[\binom{k}{j} x^{k-j} \pi^{j(n-er)} t^j \right] \geq er + j(n-er).$$

Hence, the binomial term is divisible by π^{n+1} if $n+1 \leq er + j(n-er)$, or equivalently if $n \geq er + 1/(j-1)$. By assumption $j \geq 2$ therefore $\dfrac{1}{j-1} \leq 1 \leq \left\lceil \dfrac{e+1}{p-1} \right\rceil$. Thus the lemma is still true.

When $1 \leq i < r$ then

$$\nu_\pi \left[\binom{k}{j} x^{k-j} \pi^{j(n-er)} t^j \right] \geq e(r-i) + j(n-er) \geq e(r-i) + p^i(n-er).$$

and the binomial term is divisible by π^{n+1} if

$$e(r-i) + p^i(n-er) = p^i n - ei + er(1-p^i) \geq n+1.$$

That is,

$$n \geq er + \frac{ei+1}{p^i-1}.$$

Similar to the previous case, we have (since $i \geq 1$)

$$\frac{ei+1}{e+1} = i + \frac{1-i}{e+1} \leq i \leq \frac{p^i-1}{p-1}.$$

which is equivalent to the inequality,

$$\frac{ei+1}{p^i-1} \leq \frac{e+1}{p-1}.$$

Again the lemma holds for $n \geq er + \dfrac{e+1}{p-1}$.

The inequality for $r = 0$ follows immediately since $j \geq 2$. □

Theorem 3.2.1. *Let R be a ring of integers and $\mathcal{P}$ a prime ideal in R lying over the rational prime p with ramification index e. Let $R_{\mathcal{P}}$ be the localization of R at $\mathcal{P}$, and let π be a uniformizer. Suppose $\pi^n \| k$, with $n \geq 0$.*

a) If $n \geq 1$ then for any $m \geq n + \left\lceil \frac{e+1}{p-1} \right\rceil$, if the congruence

$$\alpha \equiv x_1^k + x_2^k + \cdots + x_s^k \pmod{\mathcal{P}^m} \tag{3.7}$$

has a primitive solution $x_1, x_2, \ldots, x_s$ in R, then the congruence

$$\alpha \equiv x_1^k + x_2^k + \cdots + x_s^k \pmod{\mathcal{P}^{m+1}} \tag{3.8}$$

also has a primitive solution $x_1', x_2', \ldots, x_s'$ in R, with $x_i' \equiv x_i \pmod{\mathcal{P}^m}$, $1 \leq i \leq s$.

b) If $n = 0$ then for $m \geq 1$ if the congruence (3.7) has a primitive solution, then the congruence (3.8) also has a primitive solution satisfying the same condition.

Observations.

1. Notice that since $\left\lceil \frac{e+1}{p-1} \right\rceil \leq er = n$, Theorem 3.2.1 is an improvement on Stemmler's [30, Theorem 5] where m needed to be at least $2n+1$ in order to perform the lifting. Also note that the $(+)$ signs in (3.7) or in (3.8) could be replaced by $(\pm)$ and the Theorem will still be true.

2. $\frac{e+1}{p-1} \leq 1$ when $p > e+1$. Consequently, Lemma 3.2.1 and hence the theorem holds for $m \geq n+1$ when $p > e+1$.

3. If no primitive solution for the congruence in (3.7) is available, then we can find a primitive solution for the congruence with $\alpha - 1$ in place of α, and then add 1.

Proof of Theorem 3.2.1. Say $k = p^r k_1$ with $p \nmid k_1$, so that $n = er$. Suppose that $n \geq 1$, so that $r \geq 1$. Let m be any positive integer, $m \geq n + \left\lceil \frac{e+1}{p-1} \right\rceil$, and assume that $(x_1, x_2, \ldots, x_s)$ is a primitive $s-$tuple satisfying

$$x_1^k + x_2^k + \cdots + x_s^k \equiv \alpha \pmod{\mathcal{P}^m}. \tag{3.9}$$

After reordering we can assume that $gcd(x_1, \mathcal{P}) = 1$. Pick $\pi \in \mathcal{P} - \mathcal{P}^2$ and consider the congruence

$$(x_1 + t\pi^{m-n})^k + x_2^k + \cdots + x_s^k \equiv \alpha \pmod{\mathcal{P}^{m+1}},$$

that is,

$$(x_1^k + x_2^k + \cdots + x_s^k - \alpha) + (kx_1^{k-1}\pi^{m-n})t + \tag{3.10}$$

$$\binom{k}{2} x_1^{k-2}\pi^{2(m-n)}t^2 + \cdots + (t\pi^{m-n})^k \equiv 0 \pmod{\mathcal{P}^{m+1}}.$$

On the left-hand side of the last congruence we have $(x_1^k + x_2^k + \cdots + x_s^k - \alpha) \in \mathcal{P}^m$, $(kx_1^{k-1}\pi^{m-n}) \in \mathcal{P}^m - \mathcal{P}^{m+1}$.

By Lemma 3.2.1 the remaining terms of the binomial expansion will vanish $\pmod{\mathcal{P}^{m+1}}$. Hence, we are left with a linear congruence in t,

$$(x_1^k + x_2^k + \cdots + x_s^k - \alpha) + (kx_1^{k-1}\pi^{m-n})t \equiv 0 \pmod{\mathcal{P}^{m+1}}. \tag{3.11}$$

By Lemma 3.1.2, $R/\mathcal{P}^{n+1}$ is isomorphic to $R_{\mathcal{P}}/\mathcal{P}_{\mathcal{P}}^{m+1}$, and by choosing $\pi \in \mathcal{P} - \mathcal{P}^2$, so that π is a generator of the unique maximal ideal $\mathcal{P}_{\mathcal{P}}$ in $R_{\mathcal{P}}$ the congruence (3.11) is equivalent to the equation

$$(x_1^k + x_2^k + \cdots + x_s^k - \alpha) + (kx_1^{k-1}\pi^{m-n})t = \lambda\pi^{m+1}, \tag{3.12}$$

over the local ring $R_{\mathcal{P}}$ for some λ. Since $(x_1^k + x_2^k + \cdots + x_s^k - \alpha) \in \mathcal{P}^m$, then $\pi^m | (x_1^k + x_2^k + \cdots + x_s^k - \alpha)$, that is $(x_1^k + x_2^k + \cdots + x_s^k - \alpha) = \upsilon_1\pi^m$ for some $\upsilon_1 \in R_{\mathcal{P}}$. Similarly $(kx_1^{k-1}\pi^{m-n}) = \upsilon_2\pi^m$, for some υ_2 in $R_{\mathcal{P}}$ with $\pi \nmid \upsilon_2$. Thus we have

$$\upsilon_1\pi^m + \upsilon_2\pi^m t = \lambda\pi^{m+1},$$

$$\upsilon_2\pi^m t = (\lambda\pi - \upsilon_1)\pi^m.$$

Cancelling π^m from both sides we obtain the linear congruence

$$\upsilon_2 t \equiv -\upsilon_1 \pmod{\pi},$$

which is solvable for t, since $\pi \nmid v_2$.

If $n = 0$ then for any $m \geq 1$, each of the terms in the sum

$$\sum_{j=2}^{k} \binom{k}{j} x_1^{k-j} \pi^{j(m-n)} t^j$$

are divisible by at least π^2. Thus the same argument holds.

□

The following definition and theorem were given by R. Stemmler in [30], and are listed here for completeness purposes.

Definition 3.2.2. *[30, Stemmler] Let $\mathcal{P}$ be a prime ideal of R, such that $\mathcal{P}^\lambda \| k!$.*

I) We define $R_k(\mathcal{P})$ to be the set of elements α in R such that for any positive integer j the congruence

$$\alpha \equiv \pm x_1^k(j) \pm x_2^k(j) \pm \cdots \pm x_s^k(j) \pmod{\mathcal{P}^j}$$

has a solution $x_1(j), x_2(j), \ldots, x_s(j)$ in R for some positive integer s depending on α and j.

II) we also define $R'_k(\mathcal{P})$ to be the set of elements α in R such that the congruence

$$\alpha \equiv \pm x_1^k \pm x_2^k \pm \cdots \pm x_s^k \pmod{\mathcal{P}^\lambda}$$

has a solution $x_1, x_2, \cdots, x_s$ in R for some positive integer s depending on α.

Both $R_k(\mathcal{P})$ and $R'_k(\mathcal{P})$ are actually subrings of R.

Note that, if α is an element in $R_k(\mathcal{P})$, then we know that the congruence

$$\alpha \equiv x_1^k + x_2^k + \cdots + x_s^k \pmod{\mathcal{P}^{c+\lceil (e+1)/(p-1) \rceil}}$$

where $\mathcal{P}^c \| k$, has a solution. Therefore, by the lifting theorem, Theorem 3.2.1, we deduce that the congruence

$$\alpha \equiv \pm x_1^k \pm x_2^k \pm \cdots \pm x_s^k \pmod{\mathcal{P}^\lambda}$$

has a solution $x_1, x_2, \cdots, x_s$ in R. Hence, $\alpha \in R'_k(\mathcal{P})$, and therefore

$$R_k(\mathcal{P}) \subseteq R'_k(\mathcal{P}).$$

Theorem 3.2.2. *[30, Stemmler, Theorem 6.] Let* $k! = \mathcal{P}_1^{\lambda_1}\mathcal{P}_2^{\lambda_2}\cdots\mathcal{P}_j^{\lambda_j}$ *where* $\mathcal{P}_a \neq \mathcal{P}_b$ *whenever* $a \neq b$. *Then*

$$R_k = \bigcap_{\mathcal{P}|k!} R_k(\mathcal{P}) = \bigcap_{\mathcal{P}|k!} R'_k(\mathcal{P}), \tag{3.13}$$

and if

$$\alpha \equiv x_1^k(i) + x_2^k(i) + \cdots + x_r^k(i) - x_{r+1}^k(i) - x_{r+2}^k(i) - \cdots - x_s^k(i) \pmod{\mathcal{P}^{\lambda_i}} \tag{3.14}$$

has a solution $x_1(i), x_2(i), \cdots, x_r(i), \cdots, x_s(i)$ *in* R *for* $i = 1, 2, \cdots, j$ *and every* α *in* R, *then* $\delta(k, (k!)) \leq s$.

As noted in [30], Theorems 3.2.1, and 3.2.2 outline a method to find upper bounds for $\delta(k, (k!))$ and $\gamma(k, (k!))$. Essentially, we need to consider congruences of two types. The first type is a congruence of the form

$$\alpha \equiv x_1^k + x_2^k + \cdots + x_s^k \pmod{\mathcal{P}},$$

for every prime ideal $\mathcal{P}$ of R that divides $k!$ but does *not* divide k. The second type is a congruence of the form

$$\alpha \equiv x_1^k + x_2^k + \cdots + x_s^k \pmod{\mathcal{P}^n},$$

for every prime ideal $\mathcal{P}$ of R dividing k, such that $\mathcal{P}^c$ is the highest power of $\mathcal{P}$ that divides k, and $n = c + \left\lceil \dfrac{e+1}{p-1} \right\rceil$.

As at the beginning of this chapter, let k be a fixed positive integer, and let $\mathcal{P}$ be a prime ideal in the ring of integers R. Assume that $\mathcal{P}$ lies over the rational prime p, say $k = p^r k_1$, and has ramification index $e \geq 1$. Let $f \geq 1$ be its degree of inertia. Put $n = er$ so that $\mathcal{P}^n \| (k)$, and put $q = p^f$.

To find $\delta_R(k, P^m)$, we wish to solve the equation

$$\pm x_1^k \pm x_2^k \pm \cdots \pm x_s^k = \overline{\alpha},$$

over the residue ring $R/\mathcal{P}^m$ with s being minimal. Notice that, by The Hensel lifting in Theorem 3.2.1 we need only to consider congruences modulo $\mathcal{P}^{n+1}$ when $p > e+1$ and modulo $\mathcal{P}^{n+\lceil (e+1)/(p-1)\rceil}$ otherwise.

From Lemma 3.1.2, $R/\mathcal{P}^{n+1}$ is isomorphic to $R_{\mathcal{P}}/{\mathcal{P}_{\mathcal{P}}}^{n+1}$, and $R_{\mathcal{P}}$ is a local ring with unique maximal ideal $\mathcal{P}_{\mathcal{P}}$. In fact $R_{\mathcal{P}}$ is a discrete valuation ring. Hence there exists an element $\pi \in \mathcal{P}_{\mathcal{P}} - {\mathcal{P}_{\mathcal{P}}}^2 \subset R_{\mathcal{P}}$, such that $(\pi) = \mathcal{P}_{\mathcal{P}}$, and we can write $R_{\mathcal{P}}/{\mathcal{P}_{\mathcal{P}}}^{n+1} = R_{\mathcal{P}}/(\pi^{n+1})$. Also note that $R_{\mathcal{P}}/(\pi)$ is isomorphic to $\mathbb{F}_q$ the finite field with $q = p^f$ elements. Moreover, since the k-th powers modulo $\mathcal{P}^{n+1}$ are actually d-th powers where

$$\begin{aligned} d &= gcd(k, q^n(q-1)) \\ &= p^r gcd(k_1, (q-1)), \end{aligned}$$

and since $gcd(k_1, p) = 1$, then we can assume that $k = p^r k_1$ with k_1 dividing $(q-1)$.

Next, we generalize Lemma 2.2.4 of chapter 2, but to prove it we need the following lemma.

Lemma 3.2.2. *Let R be a ring of integers in a number field F, and $\mathcal{P}$ be a prime ideal of R. Let $R_{\mathcal{P}}$ be the localization of R at $\mathcal{P}$, and let $(\pi) = \mathcal{P}_{\mathcal{P}}$ be the unique maximal of $R_{\mathcal{P}}$. Then for any integer $m \geq 1$, any element in $R_{\mathcal{P}}$ is congruent to a unique element of the form $u + v\pi^m \pmod{(\pi^{m+1})}$, where $u \in R_{\mathcal{P}}$ runs through a complete set of representatives of residue classes in $R_{\mathcal{P}}/(\pi^m)$, and $v \in R_{\mathcal{P}}$ runs through a complete set of representatives of residue classes in $R_{\mathcal{P}}/(\pi)$.*

Proof. Since $|R_{\mathcal{P}}/(\pi)| = q$ we have q^m choices for u, and q choices for v, and so altogether q^{m+1} elements of the form $u + v\pi^m$. Thus all that remains is to show that these elements are distinct $\pmod{(\pi^{m+1})}$.

Assume that there exists $u_1 + v_1\pi^m, u_2 + v_2\pi^m$ as above such that

$$u_1 + v_1\pi^m \equiv u_2 + v_2\pi^m \pmod{(\pi^{m+1})}.$$

Hence $u_1 - u_2 + (v_1 - v_2)\pi^m = \lambda\pi^{m+1}$ for some $\lambda \in R_{\mathcal{P}}$. Thus $u_1 - u_2 = \pi^m(\lambda\pi - (v_1 - v_2))$, and so $\pi^m | (u_1 - u_2)$, that is $u_1 \equiv u_2 \pmod{(\pi^m)}$. But since u_1 and u_2 were chosen from a complete set of distinct representatives of residue classes in $R_{\mathcal{P}}/(\pi^m)$, we must have $u_1 = u_2$. This implies that $v_1 \equiv v_2 \pmod{(\pi)}$, and again by choice of the v's, we have $v_1 = v_2$ in $R_{\mathcal{P}}$. □

Theorem 3.2.3. *Let k be a fixed positive integer, and let $\mathcal{P}$ be a prime ideal in the ring of integers R. Assume that $\mathcal{P}$ lies over the rational prime p, say $k = p^r k_1$ with $r \geq 1$, and has ramification index $e \geq 1$. Let $f \geq 1$ be its degree of inertia. Put $\gamma_m = \gamma(k, \mathcal{P}^m)$, in particular $\gamma_1 = \gamma(k, \mathcal{P})$. Suppose that every element in the finite field $R/\mathcal{P}$ is expressible as a sum of k-th powers. Then, for any positive integer m,*

(i) $\gamma_{m+1} \leq (2\gamma_1 + 1)\gamma_m + \gamma_1$.

(ii) $\gamma_m \leq \frac{1}{2}[(2\gamma_1 + 1)^m - 1]$.

A stronger form of this theorem is given in Theorem 3.2.4 for the case where $p > e + 1$.

Note that by Lemma 3.1.2, $\gamma_m = \gamma(k, \mathcal{P}^m)$ is the smallest positive integer s such that every element in $R_{\mathcal{P}}/(\pi^m)$ is a sum of s k-th powers. In particular, for γ_1 we will be considering the finite field $R_{\mathcal{P}}/(\pi) = \mathbb{F}_q$ of $q = p^f$ elements. Also note that the statement "sums of k-th powers" can be replaced by "sums of $\pm$ k-th powers" and the proof will remain the same.

Proof. The proof is very close to the proof of Lemma 2.2.4 of chapter 2. Let $\gamma_m = s$. If $\gamma_{m+1} = s$, then (i) holds, otherwise, the set of all sums of $(s+1)$ k-th powers in $R_{\mathcal{P}}/(\pi^{m+1})$ has larger cardinality than the set of all sums of s k-th powers, and so there exists an element $\lambda \in R_{\mathcal{P}}/(\pi^{m+1})$ that is expressible as a sum of $(s+1)$ k-th powers, but not as a sum of s k-th powers $\pmod{\pi^{m+1}}$. Say,

$$\lambda \equiv \sum_{i=1}^{s+1} a_i^k \pmod{\pi^{m+1}},$$

for some $a_1, \ldots, a_{s+1} \in R_{\mathcal{P}}$. By Lemma 3.2.2, there exist u_0 and v_0 in $R_{\mathcal{P}}$ such that

$$\lambda \equiv u_0 + v_0\pi^m \pmod{\pi^{m+1}}.$$

In particular, $u_0 \equiv \sum_{i=1}^{s+1} a_i^k \pmod{\pi^m}$, that is u_0 is a sum of k-th powers $\pmod{\pi^m}$. It follows that $-u_0$ is also a sum of k-th powers $\pmod{(\pi^m)}$, and since $\gamma_m = s$, $-u_0 \equiv \sum_{i=1}^{s} b_i^k \pmod{\pi^m}$, for some $b_1, \ldots, b_s \in R_{\mathcal{P}}$.

By our assumption on λ, $\pi \nmid v_0$ (since otherwise λ is expressible as a sum of at most s k-th powers $\pmod{\pi^{m+1}}$), and we see that $v_0\pi^m$ is a sum of $(2s+1)$ k-th powers $\pmod{\pi^{m+1}}$. Now, by Lemma 3.2.2 every element of $R_{\mathcal{P}}/(\pi^{m+1})$ is of the form $u + \pi^m v_0 v$ where u runs through a complete set of representatives of elements in $R_{\mathcal{P}}/(\pi^{m-1})$, and v runs through a complete set of representatives of $R_{\mathcal{P}}/(\pi)$. We choose the representatives u and v such that the following holds. If $\overline{u}$ is a sum of k-th powers $\pmod{\pi^m}$ then we choose u to be a sum of at most s k-th powers of elements of $R_{\mathcal{P}}$. Since $u + \pi^m v_0 v$ is a sum of k-th powers $\pmod{\pi^{m+1}}$ then u is a sum of k-th powers $\pmod{\pi^m}$, and so it is a sum of at most s k-th powers in $R_{\mathcal{P}}$. Moreover, by our assumption that every element of $R/\mathcal{P}$ is a sum of k-th powers, the representative v can be chosen to be the sum of at most γ_1 k-th powers in $R_{\mathcal{P}}$.

Thus we conclude that

$$\gamma_{m+1} \leq s + (2s+1)\gamma_1 = s(2\gamma_1 + 1) + \gamma_1 = \gamma_m(2\gamma_1 + 1) + \gamma_1. \tag{3.15}$$

As in the proof of Lemma 2.2.4, the inequality in part (ii) follows easily by induction on m. The case $m = 1$ is trivial. Assuming the result for m, we have

$$\gamma_{m+1} \leq \gamma_m(2\gamma_1 + 1) + \gamma_1 \leq \frac{1}{2}[(2\gamma_1 + 1)^m - 1](2\gamma_1 + 1) + \gamma_1 = \frac{1}{2}[(2\gamma_1 + 1)^{m+1} - 1].$$

□

Corollary 3.2.1. *Let R and $\mathcal{P}$ be as before. Let $\nu = er + \varepsilon$, where*

$$\varepsilon = \begin{cases} 1 & \text{if } p > e+1, \\ \left\lceil \frac{e+1}{p-1} \right\rceil & \text{if } p \leq e+1. \end{cases}$$

Assume that every element in $R/\mathcal{P}$ is expressible as a sum of k-th powers. Then for any positive integer m,

$$\gamma(k, \mathcal{P}^m) \leq \frac{1}{2}[(2\gamma(k, \mathcal{P}) + 1)^{\min\{\nu, m\}} + 1].$$

Proof. If $m \leq \nu$ the result follows immediately from Theorem 3.2.3 (ii). If $m > \nu$, then follows from Theorem 3.2.1. Indeed if α has a primitive representation as a sum of k-th powers $\pmod{\mathcal{P}^\nu}$ then it does $\pmod{\mathcal{P}^m}$. On the other hand, if α does not have a primitive representation as a sum of k-th powers $\pmod{\mathcal{P}^\nu}$, then we find a primitive representation for $\alpha - 1$ as a sum of k-th powers $\pmod{\mathcal{P}^\nu}$ and by Theorem 3.2.1 $\alpha - 1$ has a primitive representation as a sum of k-th powers $\pmod{\mathcal{P}^m}$, then add 1.

□

Definition 3.2.3. *Let R be the ring of integers in a number field F and $\mathcal{P}$ be a prime ideal in R. For any positive integers m, and k define ${}_m\mathcal{A}_k$ to be the subset of $R_\mathcal{P}$ given by*

$${}_m\mathcal{A}_k = \left\{\alpha \in R_\mathcal{P} \mid \alpha \equiv x_1^k + x_2^k + \cdots + x_s^k \pmod{\pi^m}, \text{ for some } x_1, x_2, \ldots, x_s \in R_\mathcal{P}, s \in \mathbb{N}\right\}.$$

Notice that, it follows directly from Lemma 3.1.1 that the set of sums of k-th powers in $R_\mathcal{P}/\mathcal{P}_\mathcal{P}^m$ is a subring (since it is closed under multiplication, addition and additive inverses). Since ${}_m\mathcal{A}_k$ is the inverse image of this subring under the canonical mapping $R_\mathcal{P} \longrightarrow R_\mathcal{P}/{\mathcal{P}_\mathcal{P}}^m$, ${}_m\mathcal{A}_k$ is a subring of $R_\mathcal{P}$.

The next lemma was proved by Ramanujam in [24].

Lemma 3.2.3. *[24, Ramanujam, Lemma 3.] Let $\mathcal{C}$ be a commutative ring, $\mathfrak{A}$ an ideal of $\mathcal{C}$, and $s \geq 0$ a rational integer. We denote by $\mathfrak{A}^{(p^s)}$ the set of p^s-th powers of elements in $\mathfrak{A}$, and by $\mathfrak{A}_s$ the set of elements in $\mathcal{C}$ of the form $a_0 + pa_1 + \cdots + p^s a_s$ with $a_i \in \mathfrak{A}^{(p^{s-i})}$. Let $\mathcal{C}_s$ be defined from $\mathcal{C}$ as $\mathfrak{A}_s$ is defined from $\mathfrak{A}$. Then $\mathcal{C}_s$ is a subring of $\mathcal{C}$, and $\mathfrak{A}_s$ is an ideal of C_s. If $x, y \in \mathcal{C}$, with $x \equiv y \pmod{\mathfrak{A}}$, then $x^{p^s} \equiv y^{p^s} \pmod{\mathfrak{A}_s}$.*

Proof. The case $s = 0$ is trivial, so we may assume that $s \geq 1$, and that the lemma holds with $s - 1$ instead of s. Since $\mathcal{C}_s = \mathcal{C}^{(p^s)} + p\mathcal{C}_{s-1}$, the inclusions $\mathcal{C}_s.\mathcal{C}_s \subseteq \mathcal{C}_s$ and $p\mathcal{C}_{s-1} + p\mathcal{C}_{s-1} \subseteq p\mathcal{C}_{s-1}$ are trivial, and only the inclusion $\mathcal{C}^{(p^s)} + \mathcal{C}^{(p^s)} \subseteq \mathcal{C}_s$ remains to be verified. For $x, y \in \mathcal{C}$, we have

$$x^{p^s} + y^{p^s} = (x + y)^{p^s} - \sum_{0<i<p^s} \binom{p^s}{i} x^i y^{p^s - i}, \tag{3.16}$$

and if $p^l \| i$, $p^{s-l} \| \binom{p^s}{i}$, and hence by induction, $-\sum_{0<i<p^s} \binom{p^s}{i} x^i y^{p^s-i}$ belongs to $p\mathcal{C}_{s-1}$, and the right side belongs to $\mathcal{C}_s$. Thus $\mathcal{C}_s$ is a ring and $\mathfrak{A}_s$ a subring of $\mathcal{C}_s$, and clearly $\mathcal{C}_s\mathfrak{A}_s \subseteq \mathfrak{A}_s$. Finally, if $z = x + y$ with $y \in \mathfrak{A}$, if follows from (3.16) that $x^{p^s} \equiv z^{p^s} \pmod{\mathfrak{A}_s}$, which completes the proof of the lemma. □

Lemma 3.2.4. *Let $k = p^r k_1$ with $r \geq 1$ and $gcd(k_1, p) = 1$. Let $\mathcal{P}$ be a prime ideal in R such that $\mathcal{P}$ lies over the rational prime p. Also, let $\mathcal{A}_k$ and $\mathcal{A}_{k_1}$ be the subrings of $R_\mathcal{P}$ generated by sums of k-th powers and k_1-th powers of elements in $R_\mathcal{P}$ respectively. Then the set*

$$\mathfrak{N} = \left\{ (x_0^{p^r} + px_1^{p^{r-1}} + \cdots + p^r x_r) \in R_\mathcal{P} \mid x_i \in \mathcal{A}_{k_1} \text{ for } i = 0, 1, \ldots, r \right\}$$

is a subring of $R_\mathcal{P}$ and $\mathcal{A}_k \subseteq \mathfrak{N}$.

Proof. Since $\mathfrak{N} = (\mathcal{A}_{k_1})_r$ it follows from Lemma 3.2.3 that $\mathfrak{N}$ is a subring of $\mathcal{A}_{k_1}$ and hence a subring of $R_\mathcal{P}$. Now, if $x^k = \left(x^{k_1}\right)^{p^r} \in \mathcal{A}_k$ then $x^k \in \mathfrak{N}$. Since $\mathfrak{N}$ is a subring, it is closed under addition and multiplication. Therefore, $\mathcal{A}_k \subseteq \mathfrak{N}$. □

Lemma 3.2.5. *Let $\mathcal{P}$ be a prime ideal in the ring of integers R lying over the rational prime p with ramification index $e \leq p - 1$. Let $k = p^r k_1$ with $r \geq 1$, $gcd(k_1, p) = 1$ and let $n = er$. Then for any $v \in R_\mathcal{P}$ with $\pi \nmid v$, and any positive integer $j \leq n$, $v\pi^j \in {}_{(n+1)}\mathcal{A}_k$ only if $e|j$.*

Proof. Let $v\pi^j \in {}_{(n+1)}\mathcal{A}_k$ with $\pi \nmid v$. By the Ramanujam representation of sums of k-th powers and Lemma 3.2.4 we have

$$v\pi^j \equiv x_0^{p^r} + px_1^{p^{r-1}} + \cdots + p^r x_r \pmod{\pi^{n+1}}, \tag{3.17}$$

where $x_i \in {}_{(n+1)}\mathcal{A}_{k_1}$ for all $i = 0, 1, \ldots, r$. Since $n = er$ and $\pi^e | p$, say $p = u\pi^e$ with $\pi \nmid u$.

Notice that for $l = 0, 1, \ldots, r$,

$$p^{r-l} \geq (e+1)^{r-l} \geq (r-l)e + 1.$$

Therefore if $\pi | x_l$ then

$$\nu_\pi(p^l x_l^{p^{r-l}}) \geq le + p^{r-l} \geq er + 1 = n + 1,$$

where ν_π is as defined in the proof of Lemma 3.2.1. Hence, $p^l x_l^{p^{r-l}} \equiv 0 \pmod{\pi^{n+1}}$. Thus, in (3.17) let i be the minimal with $\pi \nmid x_i$. Then

$$v\pi^j \equiv p^i w \pmod{\pi^{n+1}} \tag{3.18}$$

for some $w \in R_\mathcal{P}$ with $\pi \nmid w$.

Since $v\pi^j \in R_\mathcal{P}$, we have

$$v\pi^j \equiv a_0 + a_1\pi + \cdots + a_{ei}\pi^{ei} + \cdots + a_n\pi^n \pmod{\pi^{n+1}}, \tag{3.19}$$

where $\pi \nmid a_\lambda$ for $\lambda = 0, 1, \ldots, n$, and a_λ's are uniquely determined. Therefore, from (3.18), (3.19) and by the uniqueness of the representation, we must have $j = ei$.

□

Theorem 3.2.4. *Let $\mathcal{P}$ be a prime ideal in the ring of integers R such that $\mathcal{P}$ lies over the rational prime p. Let e be the ramification index of $\mathcal{P}$ and f be the degree of inertia. Let $k = p^r k_1$ with $r \geq 1$ and $gcd(k_1, p) = 1$. Let $p^f = q$, $n = er$, and assume $k_1|(q-1)$. Assume also that $p > e+1$ and that every element in the finite field $R/\mathcal{P}$ is expressible as a sum of k-th powers. Put $\gamma_m = \gamma(k, \mathcal{P}^m)$. In particular $\gamma_1 = \gamma(k, \mathcal{P})$. Then, for any positive integer m,*

(i) $\gamma_{m+1} = \gamma_m$ unless $e|m$ in which case $\gamma_{m+1} \leq \gamma_m(2\gamma_1 + 1) + \gamma_1$.
(ii) $\gamma(k, \mathcal{P}^m) \leq \frac{1}{2}[(2\gamma_1 + 1)^{\lceil m/e \rceil} - 1]$.

Proof. Let $\gamma_m = s$ and assume that $\gamma_{m+1} \geq s+1$, so there exists an element $\lambda \in R_\mathcal{P}$ that is expressible as a sum of $(s+1)$ k-th powers $\pmod{\pi^{m+1}}$, but not as a sum of s k-th powers $\pmod{\pi^{m+1}}$. Say,

$$\lambda \equiv \sum_{i=1}^{s+1} x_i^k \pmod{\pi^{m+1}},$$

for some $x_1, \ldots, x_{s+1} \in R_\mathcal{P}$.

Define $\mathcal{U}$ and $\mathcal{V}$ to be a complete sets of representatives in $R_\mathcal{P}$ of the residue classes in $R_P/(\pi^m)$ and $R_\mathcal{P}/(\pi)$ respectively. We choose the representatives $u \in \mathcal{U}$ and $v \in \mathcal{V}$ such

that the following holds. If $\overline{u}$ is a sum of k-th powers in $R_{\mathcal{P}}/(\pi^m)$ then we choose u to be a sum of at most s k-th powers of elements of $R_{\mathcal{P}}$. By our assumption that every element of $R/\mathcal{P}$ is a sum of k-th powers, the representative v can be chosen to be the sum of at most γ_1 k-th powers in $R_{\mathcal{P}}$.

By Lemma 3.2.2, there exit $u_0 \in \mathcal{U}$ and $v_0 \in \mathcal{V}$ such that

$$\lambda \equiv u_0 + v_0\pi^m \pmod{\pi^{m+1}}.$$

Notice that,

$$u_0 \equiv \sum_{i=1}^{s+1} x_i^k \pmod{\pi^m},$$

that is u_0 is a sum of k-th powers $\pmod{\pi^m}$. Since the set of sums of k-th powers in $R_P/(\pi^m)$ is a subring. It follows that $-u_0$ is also a sum of k-th powers $\pmod{(\pi^m)}$, and since $\gamma_m = s$, $-u_0 \equiv \sum_{i=1}^{s} y_i^k \pmod{\pi^m}$, for some $y_1, \ldots, y_s \in R_{\mathcal{P}}$.
Thus $v_0\pi^m \equiv \lambda - u_0 \pmod{\pi^{m+1}}$ is a sum of $(2s+1)$ k-th powers $\pmod{\pi^{m+1}}$. That is $v_0\pi^m \in {}_{(m+1)}\mathcal{A}_k$, and by Lemma 3.2.5 $e|m$. Therefore, there can not exist an element such as λ. Hence, if $e \nmid m$ then $\gamma_{m+1} = \gamma_m$.

If $e|m$ then by our assumption on λ, $\pi \nmid v_0$ (since otherwise λ is expressible as a sum of at most s k-th powers $\pmod{\pi^{m+1}}$), and we see that $v_0\pi^m$ is a sum of $(2s+1)$ k-th powers $\pmod{\pi^{m+1}}$. Now, by Lemma 3.2.2 every element of $R_{\mathcal{P}}/(\pi^{m+1})$ is of the form $u + \pi^m v_0 v$ where $u \in \mathcal{U}$, and $v \in \mathcal{V}$. If $u + \pi^m v_0 v$ is a sum of k-th powers $\pmod{\pi^{m+1}}$ then u is a sum of k-th powers $\pmod{\pi^m}$, and so it is a sum of at most s k-th powers in $R_{\mathcal{P}}$, by the definition of $\mathcal{U}$. Also by the definition of $\mathcal{U}$, $(\pi^m v_0)v$ is a sum of $(2s+1)\gamma_1$ k-th powers $\pmod{\pi^{m+1}}$.

Thus we conclude that

$$\gamma_{m+1} \leq s + (2s+1)\gamma_1 = s(2\gamma_1 + 1) + \gamma_1 = \gamma_m(2\gamma_1 + 1) + \gamma_1. \tag{3.20}$$

For part (ii) we proceed by induction. From part (i) we have

$$\gamma_1 = \gamma_2 = \cdots = \gamma_{e-1} = \gamma_e$$

and

$$\begin{aligned}\gamma_{e+1} &\leq \gamma_e(2\gamma_1+1)+\gamma_1 \\ &= \gamma_1(2\gamma_1+1)+\gamma_1 \\ &= \frac{1}{2}\left[(2\gamma_1+1)^2-1\right].\end{aligned}$$

Suppose

$$\gamma_{((a-1)e+1)} \leq \frac{1}{2}\left[(2\gamma_1+1)^a-1\right].$$

Then

$$\begin{aligned}\gamma_{ae+1} &\leq \gamma_{((a-1)e+1)}(2\gamma_1+1)+\gamma_1 \\ &= \frac{1}{2}\left[(2\gamma_1+1)^a-1\right](2\gamma_1+1)+\gamma_1 \\ &= \frac{1}{2}\left[(2\gamma_1+1)^{a+1}-1\right].\end{aligned}$$

□

Corollary 3.2.2. *Let $\mathcal{P}$ be a prime ideal in the ring of integers R such that $\mathcal{P}$ lies over the rational prime p. Let e be the ramification index of $\mathcal{P}$ and f be the degree of inertia. Let $k = p^r k_1$ with $r \geq 1$ and $gcd(k_1, p) = 1$. Let $p^f = q$, $n = er$, and assume $k_1|(q-1)$. Assume also that $p > e+1$ and that every element in the finite field $R/\mathcal{P}$ is expressible as a sum of k-th powers. Then for any positive integer m,*

$$\gamma(k, \mathcal{P}^m) \leq \frac{1}{2}\left[(2\gamma(k,\mathcal{P})+1)^{\min\{r+1,\lceil m/e\rceil\}}+1\right].$$

Proof. As in the proof of Corollary 3.2.1. If $m \leq n+1$ the result follows immediately from Theorem 3.2.4 (ii), since $\left\lceil \frac{m}{e} \right\rceil \leq r+1$. If $m > n+1$, the result then follows from Theorem 3.2.1. Indeed if α has a primitive representation as a sum of k-th powers $\pmod{\mathcal{P}^{n+1}}$ then it does $\pmod{\mathcal{P}^m}$. On the other hand, if α does not have a primitive representation as a sum of k-th powers $\pmod{\mathcal{P}^{n+1}}$, then we find a primitive representation for $\alpha - 1$ as a sum of k-th powers $\pmod{\mathcal{P}^{n+1}}$ and by Theorem 3.2.1 $\alpha - 1$ has a primitive representation as a sum of k-th powers $\pmod{\mathcal{P}^m}$, then add 1.

□

3.3 The Group of Units in $R/\mathcal{P}^m$.

In this section, we let $\mathcal{P}$ be any prime ideal of the ring of integers R. Assume that $\mathcal{P}$ lies over the rational prime p, and has a ramification index $e \geq 1$, that is $\mathcal{P}^e \| p$ in R, and let $f \geq 1$ be the degree of inertia of $\mathcal{P}$. Let m be any positive integer. By Lemma 3.1.2, $R/\mathcal{P}^m$ is isomorphic to $R_{\mathcal{P}}/{\mathcal{P}_{\mathcal{P}}}^m$, and $R_{\mathcal{P}}$ is a local ring with the unique maximal ideal $\mathcal{P}_{\mathcal{P}}$. In fact, $R_{\mathcal{P}}$ is a discrete valuation ring, hence there exists an element $\pi \in \mathcal{P}_{\mathcal{P}} - {\mathcal{P}_{\mathcal{P}}}^2 \subset R_{\mathcal{P}}$, such that $(\pi) = \mathcal{P}_{\mathcal{P}}$, therefore we can write $R_{\mathcal{P}}/{\mathcal{P}_{\mathcal{P}}}^m = R_{\mathcal{P}}/(\pi^m)$. Also note that $R_{\mathcal{P}}/(\pi)$ is isomorphic to $\mathbb{F}_q$ the finite field with $q = p^f$ elements.

Note that from this point on $\overline{\alpha}$ will be our notation for the residue class $\alpha + \mathcal{I}$ in the residue ring $R/\mathcal{I}$ for any ideal $\mathcal{I}$ of R.

We know that $\big(R_{\mathcal{P}}/(\pi)\big)^*$ = the multiplicative group of units in $R_{\mathcal{P}}/(\pi)$ is cyclic. Hence there exists an element $a \in R_{\mathcal{P}}$ such that $\langle \overline{a} \rangle = \big(R_{\mathcal{P}}/(\pi)\big)^*$, which implies that

$$ord_{(\pi)}a = |\overline{a}| = \big|\big(R_{\mathcal{P}}/(\pi)\big)^*\big| = (q-1).$$

We have $a^{q-1} = 1 + b\pi$ for some b in $R_{\mathcal{P}}$. Replacing a by $a + \pi$ if necessary we may assume that $\pi \nmid b$.

Next, let G be the multiplicative group of units in $R_{\mathcal{P}}/(\pi^m)$. Let the order of a in G $(ord_{(\pi^m)}(a))$ be μ. Then $a^\mu \equiv 1 \pmod{\pi^m}$, which implies $a^\mu \equiv 1 \pmod{\pi}$. Thus $(q-1)$ is a divisor of μ. Also μ must be a divisor of $|G|$, so to find μ we need to know the order of G.

Let $U \subset R_{\mathcal{P}}$ be any set of representatives of the residue classes of $R_{\mathcal{P}}/(\pi)$, then every element $x \in R_{\mathcal{P}}/(\pi^m)$ can be uniquely represented in the form

$$x \equiv u_0 + u_1\pi + u_2\pi^2 + \cdots + u_{m-1}\pi^{m-1} \pmod{\pi^m}, \tag{3.21}$$

where $u_i \in U$ for $0 \leq i \leq m-1$. Therefore $x \in G$ if and only if $u_0 \neq 0$. Hence we have $q-1$ choices for u_0 and q choices for u_i, for $1 \leq i \leq (m-1)$, which implies that $|G| = (q-1)q^{m-1}$. Consequently $(q-1)|mu$ and $\mu|(q-1)q^{m-1}$, therefore $\mu = (q-1)p^j$ for some $0 \leq j \leq f(m-1)$.

Lemma 3.3.1. *Let $\mathcal{P}$ be a prime ideal in the ring of integers R, such that $\mathcal{P}$ lies over the rational prime p, with degree of inertia f and ramification index e. Let $\pi \in R_{\mathcal{P}}$ such that $(\pi) = \mathcal{P}_{\mathcal{P}}$. Then*

(i) For any $a \in R_{\mathcal{P}}$

$$a^{(q-1)p^j} = 1 + b\pi^{\mu},$$

where b is some element in $R_{\mathcal{P}}$ and

$$\begin{array}{ll} \mu = je + 1 & \text{if } e < p-1, \\ \mu \geq (j-1)e + p & \text{if } p \leq e \leq p(p-1), \\ \mu \geq jp & \text{if } e > p(p-1). \end{array}$$

(ii) If $p > e+1$ and $\overline{a}$ is a generator for $\left(R_{\mathcal{P}}/(\pi)\right)^*$ such that $a^{q-1} = 1 + b\pi$ for some b in $R_{\mathcal{P}}$ with $\pi \nmid b$, then

$$a^{(q-1)p^j} = 1 + c\pi^{\mu},$$

where c is some element in $R_{\mathcal{P}}$ with $\pi \nmid c$, and $\mu = je + 1$.

Proof. For any $a \in R_{\mathcal{P}}$, we have $a^{q-1} \equiv 1 \pmod{\pi}$. Thus, there exist an element $b \in R_{\mathcal{P}}$ such that

$$a^{q-1} = 1 + b\pi. \tag{3.22}$$

Next consider

$$(a^{q-1})^p = (1 + b\pi)^p = 1 + pb\pi + \sum_{j=2}^{p-1} \binom{p}{j} b^j \pi^j + b^p \pi^p$$

and p (or equivalently π^e) divides $\binom{p}{j}$ for all $2 \leq j \leq p-1$. Thus we have to consider two cases:

Case $1 : p > e + 1$.

Then there exists b_1 in $R_{\mathcal{P}}$ such that

$$(a^{q-1})^p = 1 + \pi^{e+1} b_1.$$

We proceed by induction. Assume for a given value of i,

$$(a^{q-1})^{p^{i-1}} = 1 + \pi^{(i-1)e+1} b_{i-1}$$

Then

$$\begin{aligned}(a^{q-1})^{p^i} &= (1+\pi^{(i-1)e+1}b_{i-1})^p \\ &= 1+p\pi^{(i-1)e+1}b_{i-1}+\sum_{j=2}^{p-1}\binom{p}{j}(\pi^{(i-1)e+1}b_{i-1})^j+\pi^{p(i-1)e+p}b_{i-1}^p,\end{aligned}$$

and so

$$(a^{q-1})^{p^i}=1+\pi^{ie+1}b_i$$

for some b_i.

Notice that, if the conditions in (ii) are satisfied, then b in (3.22) can be chosen so that $\pi \nmid b$. Therefore, as done above, we have $(a^{q-1})^{p^i}=1+\pi^{ie+1}b_i$ for some b_i with $\pi \nmid b_i$.

Case $2: p \leq e+1$.

In this case the previous argument will not hold, since the last term in the binomial expansion $\pi^p b^p$ is divisible by π^p at most. There exists c_1 in $R_{\mathcal{P}}$ such that $\pi \nmid c_1$ and

$$(a^{q-1})^p=1+\pi^p c_1.$$

So

$$(a^{q-1})^{p^2}=(1+\pi^p c_1)^p=1+p\pi^p c_1+\sum_{j=2}^{p-1}\binom{p}{j}(\pi^p c_1)^j+\pi^{p^2}c_1^p.$$

Except for the 1, all the terms in the binomial expansion on the right hand side are divisible by π^{α_2} where $\alpha_2=\min\{e+p,p^2\}$. Thus we can find c_2 in $R_{\mathcal{P}}$ such that

$$(a^{q-1})^{p^2}=1+\pi^{\alpha_2}c_2.$$

Next,

$$(a^{q-1})^{p^3}=(1+\pi^{\alpha_2}c_2)^p=1+p\pi^{\alpha_2}c_2+\sum_{j=2}^{p-1}\binom{p}{j}(\pi^{\alpha_2}c_2)^j+\pi^{p\alpha_2}c_2^p.$$

Letting $\alpha_3=\min\{e+\alpha_2,p\alpha_2\}$, we can find c_3 in $R_{\mathcal{P}}$ such that

$$(a^{q-1})^{p^3}=1+\pi^{\alpha_3}c_3.$$

Continuing in the same manner, we obtain

$$(a^{q-1})^{p^j}=1+\pi^{\alpha_j}c_j,$$

where $\alpha_j = \min\{e + \alpha_{j-1}, p\alpha_{j-1}\}$ and c_j is in $R_{\mathcal{P}}$. Now, if $\alpha_2 = e + p$ then $\alpha_3 = 2e + p$, and by induction $\alpha_j = (j-1)e + p$ for any j and so

$$a^{(q-1)p^j} = 1 + \pi^{(j-1)e+p}$$

On the other hand if $\alpha_2 = p^2$, or equivalently if $e \geq p(p-1)$, then notice that $\alpha_2 \geq 2p$ and therefore by induction $\alpha_j \geq jp$ for $j \geq 2$.

□

Now, we can characterize the group of units in $R_{\mathcal{P}}/\mathcal{P}_{\mathcal{P}}^m$ with the following lemma.

Lemma 3.3.2. *Let R be the ring of integers in a number field F. Let $\mathcal{P}$ be a prime ideal in R lying over the rational prime p with ramification index e. Let G be the multiplicative group of units in $R_{\mathcal{P}}/\mathcal{P}_{\mathcal{P}}^m$. Then*

$$|G| = (q-1)q^{m-1},$$

and there exists elements $\overline{a}, \overline{b}_1, \overline{b}_2, \ldots, \overline{b}_\iota$ such that the following conditions are satisfied.

(i) $G = \langle \overline{a}, \overline{b}_1, \overline{b}_2, \ldots, \overline{b}_\iota \rangle$,

(ii) ι *is minimal,*

(iii) $a \in R_{\mathcal{P}}$ *is a representative for the generator of the cyclic group of units* $\left(R_{\mathcal{P}}/\mathcal{P}_{\mathcal{P}}\right)^*$.

$$ord_{(\pi^m)}(a) = (q-1)p^\alpha,$$

where

$$\alpha = \lceil (m-1)/e \rceil = r \quad \text{when } p > e+1,$$

$$\alpha \leq \lceil (m-p)/e + 1 \rceil \quad \text{when } p \leq e \leq p(p-1),$$

$$\alpha \leq \lceil m/p \rceil \quad \text{when } e > p(p-1).$$

(iv) $ord_{(\pi^n)}(b_j) = p^{\beta_j}$, *where*

$$\beta_j \leq \begin{cases} \lceil (m-1)/e \rceil = r & \text{when } p > e+1, \\ \lceil (m-p)/e + 1 \rceil & \text{when } p \leq e \leq p(p-1), \\ \lceil m/p \rceil & \text{when } e > p(p-1). \end{cases}$$

for $j = 1, 2, \ldots, \iota$.

Proof. We can choose $\overline{a} \in R_{\mathcal{P}}/\mathcal{P}_{\mathcal{P}}^{n}$ as in the arguments preceding Lemma 3.3.1, that is $a \in R_{\mathcal{P}}$ such the $\langle \overline{a} \rangle = \big(R_{\mathcal{P}}/(\pi)\big)^{*}$. Since the group G is a finite and abelian, then by the Fundamental Theorem of Finitely Generated Abelian Groups, there exist $\overline{b}_1, \overline{b}_2, \ldots, \overline{b}_\iota$ elements in G, such that conditions (i) and (ii) are satisfied.

By Lemma 3.3.1, if $p > e + 1$ we have

$$(a^{q-1})^{p^j} = 1 + \pi^{je+1} b_j \equiv 1 \pmod{\pi^m}$$

if and only if $je + 1 \geq m$, that is $j \geq \left\lceil \dfrac{m-1}{e} \right\rceil$. Thus

$$ord_{(\pi^m)}(a) = (q-1)p^{\lceil (m-1)/e \rceil}.$$

Also, if $p \leq e \leq p(p-1)$

$$a^{\mu} = (a^{q-1})^{p^j} \equiv 1 \pmod{\pi^n}$$

if $(j-1)e + p \geq m$, that is $j \geq \dfrac{m-p}{e} + 1$, so let $\rho = \left\lceil \dfrac{m-p}{e} + 1 \right\rceil$ and we get

$$ord_{(\pi^m)}(a) \leq (q-1)p^{\rho}.$$

Next, if $e > p(p-1)$ then $(a^{q-1})^{p^j} \equiv 1 \pmod{\pi^m}$ if and only if $j \geq \left\lceil \dfrac{m}{p} \right\rceil$, that is

$$ord_{(\pi^m)}(a) \leq (q-1)p^{\lceil m/p \rceil}.$$

Furthermore, for $j = 1, 2, \ldots, \iota$, $ord_{(\pi^m)}(b_j) = p^{\beta_j}$ for some $\beta_j \leq f(m-1)$.

From Lemma 3.3.1 we have the following:

I.) $(b_j^{q-1})^{p^\beta} \equiv 1 \pmod{\pi^m}$ if $\beta e + 1 \geq m$ when $p \geq e + 1$.

II.) $(b_j^{q-1})^{p^\beta} \equiv 1 \pmod{\pi^m}$ if $(\beta - 1)e + p \geq m$ when $p \leq e \leq p(p-1)$.

III.) $(b_j^{q-1})^{p^\beta} \equiv 1 \pmod{\pi^m}$ if $\beta p \geq m$ when $p(p-1) < e$.

Since β_j is less than or equal to such β we have the desired result.

□

3.4 The set of k-th power units in $R/\mathcal{P}^{n+\varepsilon}$.

In this section we will use the notation defined at the beginning of this chapter. That is, let $\mathcal{P}$ be a prime ideal in R such that $\mathcal{P}^n \| (k)$ for some positive integer n. Also, assume that the prime ideal $\mathcal{P}$ lies over the rational prime p, and has a ramification index $e \geq 1$, and let $f \geq 1$ be the degree of inertia of $\mathcal{P}$. Furthermore, we write $k = p^r k_1$ where $gcd(p, k_1) = 1$, $r \geq 1$ so that $n = er$, and we put $q = p^f$.

As in the previous sections, let π be the *uniformizer* of the local ring $R_{\mathcal{P}}$, that is $\pi \in \mathcal{P}_{\mathcal{P}} - {\mathcal{P}_{\mathcal{P}}}^2 \subset R_{\mathcal{P}}$ such that $(\pi) = \mathcal{P}_{\mathcal{P}}$. Also, recall that from Lemma 3.1.2 $R_{\mathcal{P}}/\mathcal{P}_{\mathcal{P}} - {\mathcal{P}_{\mathcal{P}}}^n = R_{\mathcal{P}}/(\pi^n) \cong R/\mathcal{P}^n$. Therefore, for any integer $\varepsilon \geq 1$ we can write $R_{\mathcal{P}}/{\mathcal{P}_{\mathcal{P}}}^{n+\varepsilon} = R_{\mathcal{P}}/(\pi^{n+\varepsilon})$ which is isomorphic to $R/\mathcal{P}^{n+\varepsilon}$. Moreover, since the k-th powers in $R_{\mathcal{P}}/(\pi)$ are actually d-th powers where

$$d = gcd(k, q-1) = gcd(k_1, q-1),$$

we can assume that k_1 divides $(q-1)$, and set $t = \dfrac{q-1}{k_1}$.

Let G be the multiplicative group of units in $R_{\mathcal{P}}/(\pi^{n+\varepsilon})$. By replacing m with $n+\varepsilon$ in Lemma 3.3.2 we get that $G = \langle \overline{a}, \overline{b}_1, \overline{b}_2, \ldots, \overline{b}_\iota \rangle$, such that ι is minimal, and

$$ord_{(\pi^{n+\varepsilon})}(a) = (q-1)p^\alpha,$$

where

$$\alpha = \lceil (n+\varepsilon-1)/e \rceil = r \quad \text{when } p > e+1,$$

$$\alpha \leq \lceil (n+\varepsilon-p)/e+1 \rceil \quad \text{when } p \leq e \leq p(p-1),$$

$$\alpha \leq \lceil (n+\varepsilon)/p \rceil \quad \text{when } e > p(p-1).$$

Also for $j = 1, 2, \ldots, \iota$ we have $ord_{(\pi^{n+\varepsilon})}(b_j) = p^{\beta_j}$, where $\beta_j \leq \dfrac{n+\varepsilon-1}{e}$ when $p \geq e+1$.

Let G^k be the subgroup of G generated by $\left\{\overline{a}^k, \overline{b}_1^k, \overline{b}_2^k, \ldots, \overline{b}_\iota^k\right\}$,which is the subgroup of all k-th power units in $R_{\mathcal{P}}/(\pi^{n+\varepsilon})$.

Now, as seen in Section 3.2 the critical values of ε that we need to consider are

$$\varepsilon = \begin{cases} 1 & \text{if } p > e+1, \\ \\ \lceil \frac{e+1}{p-1} \rceil & \text{when } p \leq e+1. \end{cases}$$

Lemma 3.4.1. *With the notation and assumptions above, if $p > e+1$ then $G^k = \langle \overline{a}^k \rangle$, a cyclic group of order t. Otherwise,*

$$ord_{(\pi^{n+\varepsilon})}(a^k) = tp^{\mu},$$

such that

$$\mu \leq \min\{0, \rho_1 - r\} \quad \text{if } p \leq e \leq p(p-1),$$

$$\mu \leq \min\{0, \rho_2 - r\} \quad \text{if } e \geq p(p-1),$$

where $\rho_1 = \lceil (n+\varepsilon-p)/e + 1 \rceil$ and $\rho_2 = \lceil (n+\varepsilon)/p \rceil$. Also, for $j = 1, 2, \ldots, \iota$,

$$ord_{(\pi^{n+\varepsilon})}(b_j) = p^{\beta_j - \min\{\beta_j, r\}},$$

where β_j is given by $ord_{(\pi^{n+\varepsilon})}(b_j) = p^{\beta_j}$.

Proof. First, assume that $p > e+1$, so that $\varepsilon = 1$ then we have

$$\begin{aligned} ord_{(\pi^{n+\varepsilon})}(b_j^k) &= \frac{p^{\beta_j}}{gcd(k, p^{\beta_j})} \\ &= \frac{p^{\beta_j}}{gcd(p^r k_1, p^{\beta_j})} = p^{\beta_j - \min\{\beta_j, r\}} \end{aligned}$$

for $1 \leq j \leq \iota$. Since $r = \dfrac{n+\varepsilon-1}{e} \geq \beta_j$ we have $ord_{(\pi^{n+\varepsilon})}(b_j^k) = 1$.

$$\begin{aligned} ord_{(\pi^{n+\varepsilon})}(a^k) &= \frac{(q-1)p^r}{gcd(k, (q-1)p^r)} \\ &= \frac{tk}{gcd(k, tk)} = t. \end{aligned}$$

By denoting $\overline{a}^k = T$ we get $G^k = \{1, T, T^2, \ldots, T^{t-1}\}$.

Next if $p \leq e \leq p(p-1)$

$$\begin{aligned} ord_{(\pi^{n+\varepsilon})}(a^k) &= \frac{(q-1)p^{\alpha}}{gcd(k,(q-1)p^{\alpha})} \\ &= \frac{(q-1)p^{\alpha}}{gcd(p^r k_1,(q-1)p^{\alpha})} \\ &= tp^{\alpha-\min\{r,\alpha\}} \\ &= tp^{\min\{0,\alpha-r\}} \leq tp^{\min\{0,\rho_1-r\}}. \end{aligned}$$

Similarly if $e \geq p(p-1)$ then

$$ord_{(\pi^{n+\varepsilon})}(a^k) \leq tp^{\min\{0,\rho_2-r\}}.$$

Also if $e \geq p$ then as before we have

$$ord_{(\pi^{n+\varepsilon})}(b_j^k) = p^{\beta_j-\min\{\beta_j,r\}}, \qquad \text{for } 1 \leq j \leq \iota.$$

□

Notice that, T (as defined in the proof above) satisfies the congruence

$$T^t \equiv 1 \pmod{\pi^{n+\varepsilon}}$$

with t being minimal. Therefore, T can be taken to be a primitive t-th root of unity in $R_{\mathcal{P}}/(\pi^{n+\varepsilon})$.

Lemma 3.4.2. *let $\mathcal{P}$ be a prime ideal in R such that $\mathcal{P}^n \| (k)$ for some positive integer n. Assume that the prime ideal $\mathcal{P}$ lies over the rational prime p, and has a ramification index $e \geq 1$, and let $f \geq 1$ be the degree of inertia of $\mathcal{P}$. Let $k = p^r k_1$ where $gcd(p, k_1) = 1$, $r \geq 1$ so that $n = er$. Put $q = p^f$ and let $t = (q-1)/k_1$. Suppose that $e + 1 < p$ and let T be a primitive t-th root of unity modulo $\mathcal{P}^{n+1}$. Then every element in R_k is congruent to an integer linear combination of elements of the set $\left\{1, T, T^2, \ldots, T^{\phi(t)-1}\right\}$ modulo $\mathcal{P}^{n+1}$.*

Proof. Since $p > e + 1$ then

$$k = p^r k_1 \geq p^r \geq pr > er + r \geq er + 1 = n + 1.$$

Let π be the uniformizer of the local ring $R_{\mathcal{P}}$. It follows that if $u\pi \in R_{\mathcal{P}}$ is any nonunit then $(u\pi)^k \equiv 0 \pmod{\pi^{n+1}}$. Therefore, by the definition of R_k and Lemma 3.1.1, any element in R_k is congruent to a sum of elements of the set of k-th power units modulo $(\pi^{n+\varepsilon})$. Recall that $r = (n+\varepsilon-1)/e$, and by 3.4.1 any element in R_k will be congruent to a sum of elements of the set $\left\{1, T, T^2, \ldots, T^{t-1}\right\}$ modulo $\mathcal{P}^{n+\varepsilon}$, or equivalently modulo $(\pi^{n+\varepsilon})$. In other words, all elements of R_k are expressible as integer linear combinations of elements from the set $\left\{1, T, T^2, \ldots, T^{t-1}\right\}$ modulo $(\pi^{n+\varepsilon})$. Furthermore, let $\Phi_t(x)$ be the t-th cyclotomic polynomial over F, then $\Phi_t(x)$ has degree equal to $\phi(t)$, say $\phi(t) = l$, where ϕ is the Euler $\phi-$function. As in the proof of Lemma 2.3.2, $\Phi_t(T) \equiv 0 \pmod{\pi^{n+\varepsilon}}$. Therefore every element in R_k is congruent to an integer linear combination of elements of the set $\left\{1, T, T^2, \ldots, T^{l-1}\right\}$ modulo $(\pi^{n+\varepsilon})$.

Finally, with the help of Lemma 3.1.2 we have the desired result.

□

Notice that when $p \leq e$ then the set of integer linear combinations of elements from $\left\{1, T, T^2, \ldots, T^{\phi(t)-1}\right\}$ forms a subring of the ring of all elements that can expressed as sums of k-th powers modulo $\mathcal{P}^{n+1}$.

The next lemma was proven by Tornheim in [32].

Lemma 3.4.3. *Let $\mathbb{F}_1$ be the set of all elements in the finite field $R_{\mathcal{P}}/\mathcal{P}_{\mathcal{P}} = \mathbb{F}_q$ expressible as sums of k-th powers. Then $\mathbb{F}_1$ is a subfield of $\mathbb{F}_q$ with $q_1 = p^{f_1}$ elements where f_1 is a divisor of f.*

Proof. Clearly $\mathbb{F}_1$ is closed under addition and multiplication. If $0 \neq x \in \mathbb{F}_1$, then $-x = (p-1)x$ a sum of elements in $\mathbb{F}_1$ and $x^{-1} = (x^{-1})^k x^{k-1}$ a product of elements in $\mathbb{F}_1$. Thus $\mathbb{F}_1$ is a subfield of $\mathbb{F}_q$. Furthermore, $\mathbb{F}_1$ is an $\mathbb{F}_p$-vector subspace of the f-dimensional vector space $\mathbb{F}_q$. Therefore, there must exist an integer $f_1 \geq 1$ such that f_1 is the dimension of $\mathbb{F}_1$. Hence $\mathbb{F}_1$ has $q_1 = p^{f_1}$ elements, and f_1 must divide f. □

We will denote the subfield in Lemma 3.4.3 by $\mathbb{F}_{q_1}$.

Lemma 3.4.4. *Let $\overline{\tau}_1, \overline{\tau}_2, \ldots, \overline{\tau}_{f_1} \in \mathbb{F}_{q_1}$ be a set of linearly independent elements over $\mathbb{F}_p$, where the representatives $\tau_i \in R_{\mathcal{P}}$ are sums of k-th powers in $R_{\mathcal{P}}$. If for rational integers $\lambda_1, \lambda_2, \ldots, \lambda_{f_1}, m$ with $m \geq 1$*

$$\sum_{i=1}^{f_1} \lambda_i \tau_i \equiv 0 \pmod{\pi^m},$$

then

$$p^{\lceil m/e \rceil} | \lambda_i$$

for all $i = 1, 2, \ldots, f_1$.

Proof. Assume that for $\lambda_1, \lambda_2, \ldots, \lambda_{f_1}, m \in \mathbb{Z}$ with $m \geq 1$ and

$$\sum_{i=1}^{f_1} \lambda_i \tau_i \equiv 0 \pmod{\pi^m}. \tag{3.23}$$

Then, in particular,

$$\sum_{i=1}^{f_1} \lambda_i \tau_i \equiv 0 \pmod{\pi},$$

and by the assumption of the set $\{\tau_1, \tau_2, \ldots, \tau_{f_1}\}$, we have $\pi | \lambda_i$ for all $i = 1, 2, \ldots, f_1$. Furthermore, since $\lambda_i \in \mathbb{Z}$, then $\lambda_i = p\alpha_{i,1}$ for some $\alpha_{i,1} \in \mathbb{Z}$, $0 \leq i \leq f_1$. Therefore by cancelling p from both sides of (3.23) we get

$$\sum_{i=1}^{f_1} \alpha_{i,1} \tau_i \equiv 0 \pmod{\pi^{m-e}}. \tag{3.24}$$

Note that if $m \leq e$ then we are done. So we assume that $m > e$. Then (3.24) implies that

$$\sum_{i=1}^{f_1} \alpha_{i,1} \tau_i \equiv 0 \pmod{\pi}.$$

Therefore $\alpha_{i,1} = p\alpha_{i,2}$ for some $\alpha_{i,2} \in \mathbb{Z}$ for all $0 \leq i \leq f_1$. Hence $p^2 | \lambda_i$ for all $0 \leq i \leq f_1$. By cancelling p from both sides of (3.24) we get

$$\sum_{i=1}^{f_1} \alpha_{i,2} \tau_i \equiv 0 \pmod{\pi^{m-2e}}. \tag{3.25}$$

Again, if $m \leq 2e$ we are done. Otherwise, let $m = \rho e + \sigma$ for some rational integers $\rho \geq 2$ and $0 \leq \sigma < e$ such that $\sigma > 0$ if $\rho = 2$. Then by repeating the same argument $\rho - 2$ more times we get $p^{\rho} | \lambda_i$ for all $0 \leq i \leq f_1$. Put $\lambda_i = p^{\rho}\alpha_{i,\rho}$ and we have

$$\sum_{i=1}^{f_1} \alpha_{i,\rho}\tau_i \equiv 0 \pmod{\pi^{\sigma}}. \tag{3.26}$$

So if $\sigma = 0$ we are done. Otherwise, if $\sigma > 0$ then (3.26) implies that

$$\sum_{i=1}^{f_1} \alpha_{i,\rho}\tau_i \equiv 0 \pmod{\pi},$$

and again we get that $p | \alpha_{i,\rho}$ and consequently $p^{\rho+1} | \lambda_i$, for all i.

□

Consider the set $\mathcal{S} = \left\{ \sum_{i=1}^{f_1} n_i\tau_i \pmod{\pi^{n+\varepsilon}} \;\middle|\; 0 \leq n_i \leq p^{\lceil (n+\varepsilon)/e \rceil} - 1 \right\}$, as a subset of $R_{\mathcal{P}}/\mathcal{P}_{\mathcal{P}}^{n+\varepsilon}$. Notice that all elements of $\mathcal{S}$ are sums of k-th powers, also any two elements in $\mathcal{S}$ are distinct. Therefore, $|\mathcal{S}| = p^{f_1 \lceil (n+\varepsilon)/e \rceil}$. Furthermore, if $f = f_1$, that is all the elements of $R_{\mathcal{P}}/\mathcal{P}_{\mathcal{P}}$ are k-th powers, then $\mathcal{S} = R_{\mathcal{P}}/\mathcal{P}_{\mathcal{P}}^{n+\varepsilon}$.

3.5 When k is a prime integer.

Theorem 3.5.1. *Let R be the ring of integers in a number field F, and $\mathcal{P}$ be a prime ideal of R, such that $\mathcal{P}$ lies over the rational prime p. Let k be a rational prime, and assume that every element in the finite field $R/\mathcal{P}$ is expressible as a sum of k-th powers. Then for any positive integer m*

(i) If $\mathcal{P} \nmid (k)$ then $\gamma(k, \mathcal{P}^m) = \gamma(k, \mathcal{P})$.

(ii) If $\mathcal{P} \mid (k)$ (that is $k = p$), say $\mathcal{P}^e \| (k)$ and $k = p > e + 1$ then

$$\begin{aligned} &\gamma(k, \mathcal{P}^m) = 1 \quad \text{when } 1 \leq m \leq e \text{ and} \\ &\gamma(k, \mathcal{P}^m) \leq 4 \quad \text{when } 1 \leq e \leq m. \end{aligned}$$

For the case $\mathcal{P} \nmid (k)$ one can apply a number of new results due to James Cipra [11] (improving the work of Winterhof in [36], and [37]). First, if f is the degree of inertia of $\mathcal{P}$, then he proves

$$\gamma(k, \mathcal{P}) \leq 8f(k+1)^{1/f}.$$

Also he obtains the uniform bounds,

$$\gamma(k, \mathcal{P}) \leq \begin{cases} 83\sqrt{k} & \text{if } f = 1, \\ 16\sqrt{k} & \text{when } f = 2, \\ 10\sqrt{k} & \text{when } f \geq 3, \end{cases}$$

provided $\dfrac{p^f - 1}{2} \nmid k$.

Proof of Theorem 3.5.1. If k is a rational prime, we have

$$x^k + y^k \equiv (x+y)^k \pmod{kR},$$

that is every sum of k-th powers in R/kR is a k-th power, and so $\gamma(k, kR) = 1$. Hence, for $\mathcal{P} \mid (k)$, $0 < m \leq e$ we have $\gamma(k, \mathcal{P}^m) = 1$. Next, assume that $m \geq e+1$. Then by Theorem 3.2.1, if $\alpha \in R_k$ is congruent to a sum of s k-th powers $\pmod{\mathcal{P}^{e+1}}$ then α is congruent to a sum of s k-th powers $\pmod{\mathcal{P}^m}$. By Theorem 3.2.4 (i) we have,

$$\begin{aligned} \gamma(k, \mathcal{P}^{e+1}) &\leq \gamma(k, \mathcal{P}^e)(2\gamma(k, \mathcal{P}) + 1) + \gamma(k, \mathcal{P}) \\ &= 1(2+1) + 1 = 4. \end{aligned}$$

Now, assume that $\mathcal{P} \nmid (k)$, that is $e = 0$. As above, by Theorem 3.2.1, if $\beta \in R$ is congruent to a sum of $\gamma_1 = \gamma(k, \mathcal{P})$ k-th powers $\pmod{\mathcal{P}}$ then β is congruent to a sum of γ_1 k-th powers $\pmod{\mathcal{P}^m}$ for any integer $m \geq 1$.

□

3.6 The Lattice Method.

Let F be any algebraic number field, R it's ring of integers, and for a fixed positive integer k we let R_k be the subring of R generated by the k-th powers of elements of R. Furthermore, let $\mathcal{P}$ be a prime ideal of R, such that $\mathcal{P}$ lies over the rational prime p. Suppose that $\mathcal{P}$ has ramification index e and degree of inertia f and set $q = p^f$. Assume that $k = p^r k_1$ with $gcd(k_1, p) = 1$ and $\mathcal{P}^n \| k$, so that $n = er$. Put $t = (q-1)/k_1$, let π be the uniformizer of the local ring $R_{\mathcal{P}}$, and let $m \geq 1$ be any integer.

As in Lemma 2.3.1 in chapter 2, we let $\|\mathbf{v}\|_1 = \sum_{i=1}^{l} |v_i|$ for any l-th tuple $\mathbf{v} = (v_1, v_2, \ldots, v_l)$ in $\mathbb{Z}^l$. Let the set $\left\{1, T, T^2, \ldots, T^{t-1}\right\}$ be the set of the t-th roots of unity in $R_{\mathcal{P}}/\mathcal{P}_{\mathcal{P}}^m$, as in the argument leading to Lemma 3.4.2 in section 3.4. Also, the set of the t-th roots of unity in $R_{\mathcal{P}}/\mathcal{P}_{\mathcal{P}}^m$ is a subgroup of the multiplicative group of k-th power units $U_m^k = \{\tau_1, \tau_2, \ldots, \tau_i\}$ in $R_{\mathcal{P}}/\mathcal{P}_{\mathcal{P}}^m$, and the two sets are equal when $p > e + 1$.

From Lemma 3.4.2 we have that if $p > e + 1$ then any element in R_k is congruent to an integer linear combination of $\left\{1, T, T^2, \ldots, T^{\phi(t)-1}\right\} \subseteq U_m^k$ modulo $\mathcal{P}^m$.

Let $l = \phi(t)$. We have the following lemma.

Lemma 3.6.1. *Let $L : \mathbb{Z}^l \longrightarrow R_{\mathcal{P}}/\mathcal{P}_{\mathcal{P}}^m$, be the linear map given by $L(\boldsymbol{n}) = \sum_{i=0}^{l-1} n_i T^i$. Suppose $\boldsymbol{m}_0, \boldsymbol{m}_1, \ldots, \boldsymbol{m}_{l-1}$ in $\mathbb{Z}^l$ are linearly independent such that $L(\boldsymbol{m}_i) \equiv 0 \pmod{\pi^m}$ for all $i = 0, 1, \ldots, l-1$. Then for any $a \in R_k$ there exists an l-tuple $\boldsymbol{u}$, with $L(\boldsymbol{u}) \equiv a \pmod{\pi^m}$ and $\|\boldsymbol{u}\|_1 \leq \frac{1}{2} \sum_{i=0}^{l-1} \|\boldsymbol{m}_i\|_1$.*

This proof is very similar to the proof of Lemma 2.3.1.

Proof. By the paragraph preceding the lemma we know that there exists a $\mathbf{w} \in \mathbb{Z}^l$ with $L(\mathbf{w}) \equiv a \pmod{(\pi^{n+1})}$. Say $\mathbf{w} = \sum_{i=0}^{l-1} x_i \mathbf{m}_i$ for some $x_i \in \mathbb{R}$, $1 \leq i \leq l$. Now $x_i = y_i + \epsilon_i$ for some $y_i \in \mathbb{Z}$ and $\epsilon_i \in \mathbb{R}$ with $|\epsilon_i| \leq 1/2$, $0 \leq i \leq l-1$. Put $\mathbf{u} = \sum_{i=0}^{l-1} \epsilon_i \mathbf{m}_i = \mathbf{w} - \sum_{i=0}^{l-1} y_i \mathbf{m}_i$.

Then $L(\mathbf{u}) \equiv a \pmod{\pi^{n+1}}$ and $\|\mathbf{u}\|_1 \leq \frac{1}{2}\sum_{i=1}^{l-1} \|\mathbf{m}_i\|_1$. □

Now, we will assume that $p > e+1$. Hence the set of k-th power units U_m^k is the set of t-th roots of unity in $R_{\mathcal{P}}/\mathcal{P}_{\mathcal{P}}^m$ (or equivalently in $R/\mathcal{P}^m$). Otherwise the following only relates to the elements in R_k that are congruent to integer linear combinations of elements of the set of t-th roots of unity $\pmod{\pi^m}$.

Consider the linear congruence

$$\sum_{i=0}^{l-1} x_i T^i \equiv 0 \pmod{\pi^m}. \tag{3.27}$$

Note that this congruence describes the elements in the $ker(L)$, where L is the map defined in Lemma 3.6.1. This kernel forms a lattice, call it $\mathcal{L}$, with volume $vol(\mathcal{L}) = \big|Im(L)\big| = \big[\mathbb{Z}^l : ker(L)\big]$.

Let

$$B_M = \big\{(x_0, x_1, \ldots, x_{l-1}) \in \mathbb{Z}^l \big| 0 \leq x_i \leq M, i = 0, 1, \ldots, l-1\big\},$$

and notice that the image of L is the image of the subring ${}_m\mathcal{A}_k$ under the canonical mapping $R_{\mathcal{P}} \longrightarrow R_{\mathcal{P}}/(\pi^m)$. Therefore, denote $Im(L) = {}_m\overline{\mathcal{A}}_k$

$$|{}_m\overline{\mathcal{A}}_k| \Big| |R_{\mathcal{P}}/(\pi^m)| = q^m = p^{fm},$$

so $|{}_m\overline{\mathcal{A}}_k| = p^\alpha$ for some integer $0 < \alpha \leq fm$. Hence if $|B_M| = (M+1)^l > |{}_m\overline{\mathcal{A}}_k|$, then by the Box Principle there exist two distinct l-tuples $(x_0, x_1, \ldots, x_{l-1})$, and $(y_0, y_1, \ldots, y_{l-1})$ in B_M, such that

$$\sum_{i=0}^{l-1} (x_i - y_i) T^i \equiv 0 \pmod{\pi^m}.$$

Thus we take $M = |{}_m\overline{\mathcal{A}}_k|^{1/l}$, and $a_i = x_i - y_i, i = 0, 1, \ldots, l-1$. Then the l-tuple of differences $\mathbf{v}_0 = (a_0, a_1, \ldots, a_{l-1})$ is a nonzero solution of the congruence 3.27 , with

$$|a_i| \leq |{}_m\overline{\mathcal{A}}_k|^{1/l} = p^{\alpha/l} < q^{m/l} \qquad \text{for all } i = 0, 1, \ldots, l-1.$$

Let ω be a primitive t-th root on unity in $\mathbb{C}$, and let $l = \phi(t)$. Define the map $f : \mathbb{Z}^l \longrightarrow \mathbb{Z}[\omega]$, such that

$$f(x_0, x_1, \ldots, x_{l-1}) = \sum_{i=0}^{l-1} x_i \omega^i,$$

which is an injective homomorphism of $\mathbb{Z}$-modules.

Again as in the proof of Lemma 2.3.2, for $2 \leq i \leq (l-1)$, let

$$\mathbf{v}_{i-1} = f^{-1}\big(\omega^{i-1} f(\mathbf{v}_0)\big).$$

Then the $\mathbf{v}_0, \mathbf{v}_1, \ldots, \mathbf{v}_{l-1}$ form a set of linearly independent solutions of congruence 3.27, and $\|\mathbf{v}_i\|_1 \ll_t |{}_{(n+1)}\overline{\mathcal{A}}_k|^{1/l}$.

Now by Lemma 3.6.1 for any $a \in R_k$ there exists a solution to

$$\sum_{i=0}^{l-1} u_i T^i \equiv a \pmod{\pi^{n+1}}, \tag{3.28}$$

with $\sum_{i=0}^{l-1} |u_i| \leq \frac{1}{2} \sum_{i=0}^{l-1} \|\mathbf{v}_i\|_1$. Consequently

$$\delta(k, P^{n+1}) \leq \frac{1}{2} \sum_{i=0}^{l-1} \|\mathbf{v}_i\|_1,$$

and so

$$\delta(k, P^{n+1}) \ll_t |{}_{(n+1)}\overline{\mathcal{A}}_k|^{1/l} \ll_t q^{(n+1)/l}. \tag{3.29}$$

Finally since $T + T^2 + \cdots + T^{t-1} \equiv -1 \pmod{\pi^{n+1}}$ we have

$$\gamma(k, \mathcal{P}^{n+1}) \leq (t-1)\delta(k, \mathcal{P}^{n+1}) \ll_t |{}_{(n+1)}\overline{\mathcal{A}}_k|^{1/l}.$$

Hence we have proven a generalization of Lemma 2.3.2 of chapter 2.

Theorem 3.6.1. *Let $\mathcal{P}$ be a prime ideal of R lying over p, with ramification index $e \geq 1$ and degree of inertia $f \geq 1$. Let $k = p^r k_1$, with $gcd(k_1, p) = 1$ and $r \geq 1$. Let $q = p^f$, assume $k_1 | (q-1)$ and let $t = \dfrac{q-1}{k_1}$. Assume also that $e < p-1$. Then there exists a constant $c(t)$ such that for any positive integer m*

$$\begin{aligned} \gamma(k, \mathcal{P}^m) &\leq c(t) |{}_m\overline{\mathcal{A}}_k|^{1/\phi(t)} \\ &\leq c(t) q^{m/\phi(t)}, \end{aligned}$$

where ${}_m\overline{\mathcal{A}}_k$ is the subring of $R_{\mathcal{P}}/\mathcal{P}_{\mathcal{P}}{}^m$ generated by the k-th powers of elements in $R_{\mathcal{P}}/\mathcal{P}_{\mathcal{P}}{}^m$.

One can now rewrite the upper bound established in Theorem 3.6.1 in terms k.

Corollary 3.6.1. *With all assumptions and notation as in Theorem 3.6.1.*

$$\gamma(k, \mathcal{P}^m) \ll_t 3^m k^{m/\phi(t)}.$$

Proof. Since

$$q = p^f = k_1 t + 1 = \left(\frac{t}{p^r}\right) k + 1,$$

we have $p^{f+r} = kt + p^r$, or equivalently

$$p^{f+r} = k\left(t + \frac{1}{k_1}\right).$$

Therefore,

$$\begin{aligned} q^{m/\phi(t)} = p^{fm/\phi(t)} &= \left[\left[k\Big(t + \frac{1}{k_1}\Big)\right]^{1/(f+r)}\right]^{fm/\phi(t)} \\ &= \left[k\Big(t + \frac{1}{k_1}\Big)\right]^{\frac{fm}{\phi(t)(f+r)}} \\ &= k^{\frac{fm}{\phi(t)(f+r)}} \left(t + \frac{1}{k_1}\right)^{\frac{fm}{\phi(t)(f+r)}}. \end{aligned}$$

Now, since $\dfrac{f}{(f+r)} \leq 1$, and $\left(t + \dfrac{1}{k_1}\right)^{1/\phi(t)} \leq (t+1)^{1/\phi(t)} \leq 3$, the desired inequality follows directly from Theorem 3.6.1. □

Now we can prove the following generalization of Theorem 2.3.4 of Chapter 2.

Theorem 3.6.2. *Let $\mathcal{P}$ be a prime ideal of R lying over p, with ramification index $e \geq 1$ and degree of inertia $f \geq 1$. Let $k = p^r k_1$, with $gcd(k_1, p) = 1$ and $r \geq 1$, so that $\mathcal{P}^n \| k$ with $n = er$. Let $q = p^f$, assume $k_1 | (q-1)$ and set $t = \dfrac{q-1}{k_1}$. Assume also that $p > e+1$ and that every element in $R/\mathcal{P}$ is a sum of k-th powers. Then, for any positive integer h there exists a constant $C(h)$ such that if $t > C(h)$ and if $\phi(t) \geq h$, then for any integer $m \geq 1$*

$$\gamma(k, \mathcal{P}^m) \ll_h k^{f/h}.$$

Proof. By the lifting result in Theorem 3.2.1 we will consider the case where $m = n+1 = er+1$. J. Cipra in [11] and [12] obtained that for any positive integer h there exist a constant $c_h \in \mathbb{N}$ such that if $\phi(t) \geq h$ we have

$$\gamma_1 := \gamma(k, \mathcal{P}) = \gamma(k_1, \mathcal{P}) < c_h k_1^{1/h}. \tag{3.30}$$

Now by Corollary 3.2.2 we have

$$\begin{aligned} \gamma(k, \mathcal{P}^{n+1}) &\leq \frac{1}{2}\left[(2\gamma_1+1)^{\lceil (n+1)/e \rceil} + 1\right] \\ &= \frac{1}{2}\left[(2\gamma_1+1)^{r+1} + 1\right] \\ &< (3\gamma_1)^{r+1}. \end{aligned}$$

Thus by inequality (3.30)

$$\begin{aligned} \gamma(k, \mathcal{P}^{n+1}) &< 3^{r+1} c_h^{r+1} k_1^{(r+1)/h} \\ &= 3c_h k_1^{1/h} \left(3^h c_h^h k_1\right)^{r/h}. \end{aligned}$$

Set $C(h) = (3c_h)^h$. If $t \geq C(h)$ then $(3c_h)^h k_1 < p^f$, and it follows that

$$\gamma(k, \mathcal{P}^{n+1}) \leq 3c_h p^{fr/h} k_1^{1/h} < 3c_h k^{f/h}. \tag{3.31}$$

□

Chapter 4

Modified Method and Results

4.1 Introduction.

In this chapter as in Chapter 3, unless otherwise specified, we let F be any algebraic number field, R it's ring of integers, and for a fixed positive integer k we let R_k be the subring of R generated by the k-th powers of elements of R. Furthermore, let $\mathcal{P}$ be a prime ideal of R, such that $\mathcal{P}$ lies over the rational prime p. Suppose that $\mathcal{P}$ has ramification index e and degree of inertia f and set $q = p^f$. Assume that $k = p^r k_1$ with $gcd(k_1, p) = 1$, $r \geq 1$, and $\mathcal{P}^n \| (k)$, so that $n = er$. Also we assume that $k_1 | (q-1)$ and set $t = \dfrac{q-1}{k_1}$.

One can see that the method applied in Chapter 2 and generalized in Section 3.6 of Chapter 3, can be very useful to obtain upper bounds for Waring's problem over number fields when the dependence of the degree of inertia f is allowed. In other words when f is sufficiently small, and can be bounded by a constant independent of the the degree of the extension then we obtain good bounds.

If we combine our early results with the method of Stemmler from [30] we obtain an upper bound for the global case as follows. Suppose k has the prime ideal factorization

$$(k) = \mathcal{P}_1^{n_1} \mathcal{P}_2^{n_2} \cdots \mathcal{P}_m^{n_m},$$

where the $\mathcal{P}_i$ are distinct prime ideals such that $\mathcal{P}_i \bigcap \mathbb{Z} = p_i \mathbb{Z}$ with p_i a prime integer. Let f_i the degree of inertia of $\mathcal{P}_i$ for $i = 1, 2, \ldots, m$, and put $t = \max \left\{ \dfrac{p_i^{f_i} - 1}{k/p_i^{r_i}} \right\}$. Then for any

positive integer h there exists a constant $C(h)$ such that if $\phi(t) \geq h$ then

$$\begin{aligned}\gamma_R(k) &\leq 2^{k-1} + \max_{1\leq i\leq m}\left\{\gamma(k, \mathcal{P}_i^{n_i+1})\right\} \\ &\leq 2^{k-1} + \max_{1\leq i\leq m}\left\{C(h)k^{f_i/h}\right\} \\ &\leq 2^{k-1} + C(h)k^{d/h},\end{aligned}$$

where d is the degree of the extension.

Clearly, the upper bound above is not sharp. In this chapter we will modify the method used in the previous chapter to obtain sharper results.

4.2 Studying the case when $t = \dfrac{p^f - 1}{k_1} = 4$.

Theorem 4.2.1. *Let R be the ring of integers in a number field F, and $\mathcal{P}$ be a prime ideal of R, such that $\mathcal{P}$ lies over the rational prime p. Suppose that $\mathcal{P}$ has ramification index $e < p-1$ and degree of inertia f and set $q = p^f$. Assume that $k = p^r k_1$ with $gcd(k_1, p) = 1$, $r \geq 1$, and $\mathcal{P}^n \| (k)$, so that $n = er$. Also we assume that $k_1 | (q-1)$ and set $t = \dfrac{q-1}{k_1}$. Then, if $t = 4$ and m is any positive integer we have*

$$\gamma(k, \mathcal{P}^m) \leq \begin{cases} \sqrt{6k} - 1 & \text{if } p \equiv 1 \pmod 4, \\ \\ \frac{4}{p-1}k & \text{if } p \equiv 3 \pmod 4. \end{cases}$$

Moreover, for $m \geq er + 1$ we have $\gamma(k, \mathcal{P}^m) = (p^{r+1} - 1)$.

In the course of the proof we shall obtain the following lower bounds for the case $p \equiv 3 \pmod 4$, (in which case $f \geq 2$),

$$\gamma(k, \mathcal{P}^{n+1}) \geq \begin{cases} (4k)^{2/(f+1)} - 1 & \text{if } r = 1, \\ (4k)^{3/(2\max\{f,r\})} - 1 & \text{if } r \geq 2. \end{cases} \tag{4.1}$$

Proof. We shall work over the local ring $R_{\mathcal{P}}$. Let $\mathcal{P} = (\pi)$. By the lifting theorem, Theorem 3.2.1, we need only consider congruences $\pmod{\pi^{n+1}}$ where $n = er$. Furthermore, by the

assumption $p > e+1$ in the theorem we have that the set of k-th power units U_{n+1}^k in $R_{\mathcal{P}}$ modulo (π^{n+1}) is precisely the set of 4-th roots of unity $\{\pm 1, \pm T\}$

By Lemma 3.4.2, every element in R that can be expressed as a sum of k-th powers is congruent to an element in the form of $n_0 + n_1 T \pmod{\pi^{n+1}}$, where n_0, n_1 are rational integers. Also, since $(\pi^e) = (p) = pR$, the smallest positive rational integer congruent to zero modulo (π^{n+1}) is $p^{\lceil (n+1)/e \rceil}$, and $\lceil (n+1)/e \rceil = r+1$. Thus n_0 and n_1 can be chosen from the complete set of representatives $\{0, 1, \ldots, p^{r+1} - 1\}$.

Since $t = 4$, p is odd, so we can consider two cases, $p \equiv \pm 1 \pmod 4$. If $p \equiv 1 \pmod 4$ then there exist positive integers a and b, with $b < a$ and

$$a^2 + b^2 = p^{r+1} \equiv 0 \pmod{\pi^{n+1}}.$$

Since the 4-th cyclotomic polynomial $\Phi_4(x)$ satisfies the congruence $\Phi_4(T) = T^2 + 1 \equiv 0 \pmod{\pi^{n+1}}$, we have $T^2 \equiv -1 \pmod{\pi^{n+1}}$, and therefore can take $T \equiv a\bar{b} \pmod{\pi^{n+1}}$, where $\bar{b} \pmod{\pi^{n+1}}$ is the multiplicative inverse of $b \pmod{\pi^{n+1}}$.

Now we can use the same method applied in the proof of Theorem 2 in [21] which essentially follows from Lemma 3.6.1. Let $\mathcal{L}$ be the lattice in $\mathbb{Z}^2$ consisting of points (x, y) satisfying $x + yT \equiv 0 \pmod{\pi^{n+1}}$, then (a, b) and $(-b, a)$ form a basis for a sublattice $\mathcal{L}'$ of volume $vol(\mathcal{L}') = p^{r+1}$.

Let

$$\wp = \left\{ x(a,b) + y(-b,a) \mid -\frac{1}{2} < x \leq \frac{1}{2}, -\frac{1}{2} < y \leq \frac{1}{2} \right\}$$

be the the fundamental parallelogram of $\mathcal{L}'$ centered at the origin. Then $\wp$ contains p^r distinct integer points. Let $\mathcal{A}$ be the subring consisting of all the elements in $R_{\mathcal{P}}/(\pi^{n+1})$ that are expressible as sums and differences of k-th power, the mapping $\eta : \wp \cap \mathbb{Z}^2 \longrightarrow \mathcal{A}$, given by $\eta(x, y) = x + yT \pmod{\pi^{n+1}}$, is surjective by the definition of $\mathcal{A}$. η is also injective since the only point in $\wp$ mapped to zero modulo (π^{n+1}) is the origin.

Let $g : \mathbb{R}^2 \longrightarrow \mathbb{R}^+ \cup \{0\}$, be the map given by $g(x, y) = |x| + |y|$, then g restricted to $\wp$ takes on it's maximum value at the corner points

$$\pm\Big(\frac{a-b}{2},\frac{a+b}{2}\Big) \text{ and } \pm\Big(\frac{a+b}{2},\frac{b-a}{2}\Big).$$

Since p is odd, a and b are of opposite parity, so g restricted to $\wp \cap \mathbb{Z}^2$ takes on its maximum value, which is $(a-1)$, at one of the points

$$\pm\Big(\frac{a-b-1}{2},\frac{a+b-1}{2}\Big) \text{ and } \pm\Big(\frac{a+b-1}{2},\frac{b-a+1}{2}\Big).$$

Thus

$$\gamma(k,\mathcal{P}^{n+1}) \le a-1. \tag{4.2}$$

We can now obtain an upper bound for $\gamma(k,\mathcal{P}^{n+1})$ expressed in terms of k. Since

$$k = p^r k_1 = p^r \frac{p^f-1}{4},$$

hence $4k \ge p^{r+f-1}$. Therefore, if $f \ge 2$ we have $4k \ge p^{r+1} \ge a^2$, while if $f=1$ then $4k = p^{r+1}\left(\frac{p-1}{p}\right) \ge \frac{2}{3}p^{r+1}$, and so $6k \ge p^{r+1} \ge a^2$. Thus

$$\gamma(k,\mathcal{P}^{n+1}) \le \begin{cases} 2\sqrt{k}-1 & \text{when } f \ge 2\ , \\ \sqrt{6k}-1 & \text{when } f=1. \end{cases}$$

Hence, for any f

$$\gamma(k,\mathcal{P}^{n+1}) \le 3\sqrt{k}-1.$$

Next we consider the case where $p \equiv 3 \pmod 4$. Since the set of k-th power units is actually $\{\pm 1, \pm T\}$ and since T and 1 are linearly independent over $\mathbb{F}_p$, it follows from Lemma 3.4.4 that 1 and T are linearly independent over $\mathbb{Z}/p^{r+1}\mathbb{Z}$. Therefore, every element that is congruent to a sum of k-th powers is congruent to an element of the form $\pm n_0 \pm n_1 T \pmod{\pi^{n+1}}$, where n_0 and n_1 can be chosen from the set $\{0,1,2,\ldots,\frac{p^{r+1}-1}{2}\}$.

We see in particular that $\gamma(k,\mathcal{P}^{n+1}) \le 2\left(\frac{p^{r+1}-1}{2}\right) = p^{r+1}-1$. Moreover, the element $n_0+n_1T \pmod{\pi^{n+1}}$ with $n_0 = n_1 = \left(\frac{p^{r+1}-1}{2}\right)$ can not be expressed by any fewer k-th powers. Thus

$$\gamma(k,\mathcal{P}^{n+1}) = p^{r+1}-1. \tag{4.3}$$

Since $k = p^r k_1 = p^r \left(\frac{p^f - 1}{4}\right)$, that is $4k = p^{r+f}\left(1 - \frac{1}{p^f}\right)$. Hence $p^{r+f-1} \leq (4k) \leq p^{r+f}$, which implies

$$(4k)^{(r+1)/(r+f)} \leq p^{r+1} \leq (4k)^{(r+1)/(r+f-1)}.$$

Consequently

$$(4k)^{(r+1)/(r+f)} - 1 \leq \gamma(k, \mathcal{P}^{n+1}) \leq (4k)^{(r+1)/(r+f-1)} - 1. \tag{4.4}$$

Note that since $p^f \equiv 1 \pmod 4$, and $p \equiv 3 \pmod 4$, then f must be an even integer. From (4.3) and since $r \geq 1$ we have

$$\begin{aligned} \gamma(k, \mathcal{P}^{n+1}) = (p^{r+1} - 1) &= p^r(p - 1/p^r) \\ &= 4p^r k_1 \left(\frac{p - 1/p^r}{p^f - 1}\right) \\ &= 4k \left(\frac{p - 1/p^r}{(p-1)(p^{f-1} + p^{f-2} + \cdots + 1)}\right) \\ &\leq \frac{4k}{p-1} \end{aligned}$$

the last inequality following since $p^f \geq p^2$.

Now, we will obtain lower bounds for $\gamma(k, \mathcal{P}^{n+1})$ from (4.4) in terms of k, by considering the relation between $f \geq 2$ and $r \geq 1$ as follows.

Case 1. Suppose $r = 1$.

Then direct substitution in (4.4) yields

$$(4k)^{2/(f+1)} - 1 \leq \gamma(k, \mathcal{P}^{n+1}) \leq (4k)^{2/f} - 1 \leq 4k - 1. \tag{4.5}$$

Case 2. Suppose $2 \leq r \leq f$.

Then

$$\frac{r+1}{r+f} \geq \frac{3}{2f}.$$

Also

$$\frac{r+1}{r+f-1} \leq \frac{r+1}{2r-1} \leq 1.$$

Hence, we get from (4.4)

$$(4k)^{3/(2f)} - 1 \leq \gamma(k, \mathcal{P}^{n+1}) \leq 4k - 1. \tag{4.6}$$

Case 3. Suppose $2 \leq f \leq r$.

Here

$$\frac{r+1}{r+f} \geq \frac{r+1}{2r} \geq \frac{3}{2r},$$

and

$$\frac{r+1}{r+f-1} \leq \frac{r+1}{r+1} = 1.$$

Therefore, we have

$$(4k)^{3/(2r)} - 1 \leq \gamma(k, \mathcal{P}^{n+1}) \leq 4k - 1. \tag{4.7}$$

□

4.3 For an arbitrary value of $t = \dfrac{p^f - 1}{k_1}$.

A very similar approach to the one used in section 4.2 can be used for any value of t other than 4. In this section we will prove the following main result

Theorem 4.3.1. *Let R be the ring of integers in a number field F, and $\mathcal{P}$ be a prime ideal of R, such that $\mathcal{P}$ lies over the rational prime p. Suppose that $\mathcal{P}$ has ramification index $e < p-1$ and degree of inertia f and set $q = p^f$. Assume that $k = p^r k_1$ with $gcd(k_1, p) = 1$, $r \geq 1$, and $\mathcal{P}^n \| (k)$, so that $n = er$. Also we assume that $k_1 | (q-1)$ and set $t = \dfrac{q-1}{k_1}$. Then for any positive integer m*

$$\gamma(k, \mathcal{P}^m) \leq \phi(t)\gamma(k, p^{r+1}),$$

where $\gamma(k, p^{r+1})$ *is as defined in Chapter 2. Moreover,*

$$\gamma(k, \mathcal{P}^m) \leq \begin{cases} \left(\frac{p}{p-1}\right) k + 1 & \text{if } f = 1, \\ \max\left\{k, 2313 \left(\frac{k}{k_1}\right)^{(8.44)/\log p} + \frac{1}{2}\right\} & \text{if } f = 2, \text{ or } 3, \\ \max\left\{k, 129 \left(\frac{k}{k_1}\right)^{(5.55)/\log p} + \frac{1}{2}\right\} & \text{if } f \geq 4. \end{cases}$$

In particular,

$$\gamma(k, \mathcal{P}^m) \ll k \text{ for } p > 4628.6.$$

This is sharper than the result obtained by Ramanujam in [24], where he showed that

$$\gamma(k, \mathcal{P}^m) \leq 8k^5.$$

First consider the following two results

Theorem 4.3.2. *Let R be the ring of integers in an algebraic number field F, and let $\mathcal{P}$ be a prime ideal in R that lies over the rational prime p. Assume that $\mathcal{P}$ does not ramify and has a degree of inertia $f = 1$. Then for any positive integer m, $R/\mathcal{P}^m$ and $\mathbb{Z}/(p^m)$ are isomorphic as rings.*

Proof. By the assumptions we can write $\mathcal{P} = pR$ and by definition of extension rings R contains $\mathbb{Z}$, also note this result is well know for $m = 1$, so let $m \geq 2$ and the map $\theta : \mathbb{Z} \longrightarrow R/\mathcal{P}^m$ be the canonical map given by $\theta(a) = a + P^m$ in R/P^m.

One can easily show that θ is a homomorphism of rings, so we consider the kernel of θ, $ker(\theta)$, and observe that for any integer a, a belongs to $ker(\theta)$ if and only if a as an element of R belongs to $\mathcal{P}^m = p^m R$, or equivalently a is divisible by p^m. Thus $ker(\theta) = p^m\mathbb{Z}$, and by the Fundamental Theorem of Homomorphisms $\mathbb{Z}/p^m\mathbb{Z}$ is isomorphic to the image of the map θ, $Im(\theta)$.

Now, $|\mathbb{Z}/(p^m)| = |Im(\theta)| = p^m$, and the cardinality of $R/\mathcal{P}^m$ is $p^{mf} = p^m$. Therefore $Im(\theta) = R/\mathcal{P}^m$.

□

Hence when $f = e = 1$ the problem is reduced to the problem we discussed in Chapter 2. If we have $f = 1$ (and e arbitrary) we still get the following.

Theorem 4.3.3. *Let R be the ring of integers in an algebraic number field F, and let $\mathcal{P}$ be a prime ideal in R that lies over the rational prime p with ramification index e. Let $k = p^r k_1$ with $p \nmid k_1$ and $r \geq 1$, and put $n = er$. Assume that $\mathcal{P}$ has a degree of inertia $f = 1$. Let $\mathcal{A}$ be the subring consisting of sums of k-th powers in ring $R_{\mathcal{P}}/(\pi^{n+1})$. Then $\mathcal{A}$ and $\mathbb{Z}/(p^{r+1})$ are isomorphic as rings.*

Recall that $\mathcal{A}$ can be considered as the homomorphic image of R_k under the canonical epimorphism from R to $R_{\mathcal{P}}/(\pi^{n+1})$.

Proof. $f = 1$ implies that $R_{\mathcal{P}}/(\pi) \cong \mathbb{F}_p = \mathbb{Z}_p$. Any element $x \in R_{\mathcal{P}}$ is congruent to an element of the form

$$u_0 + u_1\pi + \cdots + u_n\pi^n \pmod{\pi^{n+1}}$$

where $u_i \in R_{\mathcal{P}}$ can be chosen from a complete set of representatives for the residue classes in $R_{\mathcal{P}}/(\pi)$ for all $0 \leq i \leq n$. Therefore, we have

$$R_{\mathcal{P}}/(\pi^{n+1}) = \widetilde{\mathbb{Z}}_p + \pi\widetilde{\mathbb{Z}}_p + \cdots + \pi^n\widetilde{\mathbb{Z}}_p,$$

where $\widetilde{\mathbb{Z}}_p = \{0, 1, 2, \ldots, p-1\}$ is a complete set of representatives in $R_{\mathcal{P}}$ for the residue classes in $R_{\mathcal{P}}/(\pi)$.

Furthermore, if $x \in R_{\mathcal{P}}/(\pi^{n+1})$ say,

$$\begin{aligned} x &\equiv u_0 + u_1\pi + \cdots + u_n\pi^n \pmod{\pi^{n+1}} \\ &\equiv u_0 + \pi\left(u_1 + \cdots + u_n\pi^{n-1}\right) \pmod{\pi^{n+1}} \\ &\equiv u_0 + v\pi \pmod{\pi^{n+1}}, \end{aligned}$$

we have $x^k \equiv (u_0 + v\pi)^k \pmod{\pi^{n+1}}$, that is

$$x^k \equiv u_0^k + \sum_{j=1}^{k-1} \binom{k}{j} u_0^{k-j} v^j \pi^j + v^k\pi^k \pmod{\pi^{n+1}}.$$

Since $p^r \sim \pi^{er} \mid k$ all of the terms $j = 1, 2, \ldots k-1$ vanish. Also since $p > e+1$ we have $k \geq p^r \geq pr > er+1 = n+1$ and so the last term vanishes as well. Therefore $x^k \equiv u_0^k \pmod{\pi^{n+1}}$. This implies that the subring $\mathcal{A}$ is actually generated by sums of k-th powers of the representatives $\{0, 1, 2, \ldots, p-1\}$. Thus $\mathcal{A} \subseteq \widetilde{\mathbb{Z}}_p + p\widetilde{\mathbb{Z}}_p + \cdots + p^r\widetilde{\mathbb{Z}}_p \subseteq \mathcal{A}$. That is,

$$\mathcal{A} = \widetilde{\mathbb{Z}}_p + p\widetilde{\mathbb{Z}}_p + \cdots + p^r\widetilde{\mathbb{Z}}_p.$$

Hence, $\mathcal{A}$ and $\mathbb{Z}/(p^{r+1})$ are isomorphic as rings. □

Proof of Theorem 4.3.1. By the lifting result in Theorem 3.2.1, it suffices to consider the case $m = er + 1 = n + 1$. Suppose $f = 1$, if $e = 1$ then by Theorem 4.3.2 we have the stronger results from Chapter 2 such as Theorem 2.3.1, or Theorems 2.3.2 and 2.3.3. Also if $e \geq 2$, then by Theorem 4.3.3 we have

$$\gamma(k, \mathcal{P}^{n+1}) = \gamma(k, p^{r+1}),$$

hence we still have the results from Chapter 2. In particular, from Theorem 2.2.1

$$\gamma(k, \mathcal{P}^{n+1}) \leq \left(\frac{p}{p-1}\right) k + 1.$$

Now, let $f \geq 2$. Assuming that $p > e+1$ implies that the set of t-th roots of unity $\{1, T, T^2, \ldots, T^{t-1}\}$ is precisely the set of k-th power units U_{n+1}^k in $R_{\mathcal{P}}/(\pi^{n+1})$. Hence, by Lemma 3.4.2 every element in R_k is congruent to an element of the form

$$n_0 + n_1 T + \cdots + n_{l-1} T^{l-1} \pmod{\pi^{n+1}},$$

where $n_0, n_1, \ldots, n_{l-1}$ are rational integers, and $l = \phi(t)$. Furthermore, since $p^{\lceil (n+1)/e \rceil} = p^{\lceil (er+1)/e \rceil} = p^{r+1}$ is the smallest positive integer congruent to zero modulo (π^{n+1}), then n_i can be chosen from the set $\{0, 1, \ldots, p^{r+1} - 1\}$, for $i = 0, 1, 2, \ldots, l-1$, which is the complete set of representatives of rational integers modulo (π^{n+1}). If we allow for $\pm$ then n_i can be chosen from the set $\{0, 1, \ldots, (p^{r+1} - 1)/2\}$, for $i = 0, 1, 2, \ldots, l-1$.

Thus

$$\begin{aligned}\gamma(k,\mathcal{P}^{n+1}) &\leq l\gamma(k,p^{r+1}) \\ &= \phi(t)\gamma(k,p^{r+1}) \\ &\leq \phi(t)\gamma((k,\phi(p^{r+1}),p^{r+1}),\end{aligned}$$

where $\gamma(k,p^{r+1})$ is as defined in Chapter 2. It suffices to use the trivial bound $\gamma(k,p^{r+1}) \leq p^{r+1}$ and so

$$\gamma(k,\mathcal{P}^{n+1}) \leq \phi(t)p^{r+1}.$$

We can now express the upper bound in terms of k. Since $k = p^r k_1$ then we have

$$\gamma(k,\mathcal{P}^{n+1}) \leq k, \qquad \text{if} \quad k_1/p > \phi(t).$$

Otherwise, consider $\phi(t) \geq k_1/p$. Then

$$t = \frac{(p^f-1)}{k_1} \geq \frac{(p^f-1)}{p\phi(t)},$$

that is

$$t\phi(t) \geq p^{f-1} - \frac{1}{p},$$

but the left hand side of the inequality is a rational integer, so

$$t^2 \geq t\phi(t) \geq p^{f-1}.$$

Therefore we have

$$t \geq p^{(f-1)/2}. \tag{4.8}$$

Let

$$\gamma_1 = \gamma(k,\mathcal{P}) = \gamma(k_1,\mathcal{P}), \text{ and } \gamma_{n+1} = \gamma(k,\mathcal{P}^{n+1}).$$

We use the lifting result from Corollary 3.2.2

$$\gamma_{n+1} \leq \frac{1}{2}\left[(2\gamma_1+1)^{r+1}+1\right].$$

$k = p^r k_1$ implies that $r = \log\left(\frac{k}{k_1}\right) / \log p \leq \log k / \log p$. Therefore,

$$\gamma_{n+1} \leq \frac{1}{2}(2\gamma_1 + 1)\left[(2\gamma_1 + 1)^{\log\left(\frac{k}{k_1}\right)/\log p}\right] + \frac{1}{2}. \tag{4.9}$$

Let A be a subgroup of the multiplicative group of units in $R_{\mathcal{P}}/(\pi)$ with f linearly independent points over $\mathbb{F}_p$. T. Cochrane and J. Cipra proved in [13, Corollary 6.1] that

$$\text{if } |A| \geq 1.26p^{f/3} \text{ then } \gamma_1 \leq 128,$$

$$\text{if } |A| \geq 1.17p^{2f/9} \text{ then } \gamma_1 \leq 2312.$$

We take A to be the multiplicative subgroup of k-th power units in $R_{\mathcal{P}}/(\pi)$ with $|A| = t$. If $f = 2$, then $\frac{f-1}{2} \geq \frac{2f}{9}$, therefore by (4.8) $|A| \geq 1.17p^{4/9}$ for $p \geq 17$. Similarly for $f = 3$ we have that $|A| \geq 1.17p^{2/3}$ for all $p \geq 2$. Furthermore, if $f \geq 4$ then $\frac{f-1}{2} \geq \frac{f}{3}$, which implies $|A| \geq 1.26p^{f/3}$ for $p \geq 5$. So for $f = 2, 3$ we take $\gamma_1 \leq 2312$ and we get

$$\begin{aligned}
\gamma_{n+1} &\leq 2313\left[(4625)^{\log\left(\frac{k}{k_1}\right)/\log p}\right] + \frac{1}{2} \\
&\leq 2313\left(\frac{k}{k_1}\right)^{\frac{\log(4625)}{\log p}} + \frac{1}{2} \\
&= 2313\left(\frac{k}{k_1}\right)^{(8.44)/\log p} + \frac{1}{2}.
\end{aligned}$$

If $f \geq 4$ we take $\gamma_1 \leq 128$, and get similarly

$$\gamma_{n+1} \leq 129\left(\frac{k}{k_1}\right)^{(5.55)/\log p} + \frac{1}{2}.$$

Hence by finally applying Theorem 3.2.1 and observation (2) following the theorem we have the desired result.

□

Let G be the multiplicative group $G = \mathbb{F}_q^* = (R/\mathcal{P})^*$ and $G^k = \{x^k | x \in G\}$, so that

$$|G^k| = \frac{q-1}{(q-1,k)} = \frac{q-1}{(q-1,k_1)}. \tag{4.10}$$

Using known upper bounds for γ_1 and equation (4.9), we obtain

Corollary 4.3.1. *Let R be the ring of integers in a number field F, and $\mathcal{P}$ be a prime ideal of R, such that $\mathcal{P}$ lies over the rational prime p. Suppose that $\mathcal{P}$ has ramification index $e < p-1$. Assume that $k = k_1 p^r$ with $r \geq 1$ $p \nmid k_1$, and $\mathcal{P}^n \| k$, so that $n = er$. Assume also that every element in the finite field $R/\mathcal{P}$ is expressible as a sum of k-th powers. For any δ with $0 < \delta < 1$, if $(k_1, q-1) \leq (q-1)^{1-\delta}$ then for any positive integer m,*

$$\gamma(k, \mathcal{P}^m) \leq 159\left(4^{2/\delta}\right)\left(\frac{k}{k_1}\right)^{\frac{(5.76+2.78/\delta)}{\log p}} + \frac{1}{2}.$$

Proof. Cochrane and Cipra proved, in [13],

$$\gamma_1 \leq 633(2k_1)^{\log 4/\log|G^k|}.$$

By the assumption $k_1 \leq (q-1)^{1-\delta}$, and from (4.10), we have $|G^k| \geq (q-1)^{\delta}$. Since $q-1 \geq 2$ we get

$$\begin{aligned}
\gamma_1 &\leq 633\left(2(q-1)^{1-\delta}\right)^{\frac{\log 4}{\delta \log(q-1)}} \\
&= 633\left(4^{\frac{\log 2+(1-\delta)\log(q-1)}{\delta\log(q-1)}}\right) \\
&\leq \frac{633}{4}4^{2/\delta}.
\end{aligned}$$

Therefore, from equation (4.9) we have

$$\begin{aligned}
\gamma(k, \mathcal{P}^m) &\leq \left(\frac{633}{4}4^{2/\delta} + \frac{1}{2}\right)\left(\frac{k}{k_1}\right)^{\frac{\log\left(\frac{633}{2}\left(1+\frac{1}{(8)(633)}\right)\right)+4\log 2/\delta}{\log p}} + \frac{1}{2} \\
&\leq 159\left(4^{2/\delta}\right)\left(\frac{k}{k_1}\right)^{(5.76+2.78/\delta)/\log p} + \frac{1}{2}.
\end{aligned}$$

□

In special cases, we get a sharper bound.

Corollary 4.3.2. *Under the same hypotheses as Corollary 4.3.1, for any positive integer m*

$$\gamma(k,\mathcal{P}^m) \leq \begin{cases} \frac{3}{2}\left(\frac{k}{k_1}\right)^{1.10/\log p} + \frac{1}{2} & \text{if } (k_1, q-1) = 1, \\ \frac{5}{2}\left(\frac{k}{k_1}\right)^{1.61/\log p} + \frac{1}{2} & \text{if } (k_1, q-1) \leq \frac{2}{3}q^{1/4}, \\ \frac{7}{2}\left(\frac{k}{k_1}\right)^{1.95/\log p} + \frac{1}{2} & \text{if } (k_1, q-1) \leq \frac{2}{3}q^{1/3}, \\ \frac{17}{2}\left(\frac{k}{k_1}\right)^{2.84/\log p} + \frac{1}{2} & \text{if } (k_1, q-1) \leq \frac{2}{3}q^{1/2}. \end{cases}$$

Proof. If $(k_1, q-1) = 1$ we have that $\gamma_1 = \gamma(k_1, \mathcal{P}) = \gamma(1, \mathcal{P}) = 1$. Therefore, the first inequality follows immediately from the equation (4.9). To prove the second and the third inequalities we use the following:

From the estimate of Hua and Vandiver [20], and Weil [35]

$$|N(\alpha) - q^{s-1}| \leq (k_1 - 1)^s q^{\frac{s-1}{2}},$$

for the number $N(\alpha)$ of solutions of the congruence

$$x_1^k + x_2^k + \cdots + x_s^k \equiv \alpha \pmod{\mathcal{P}}$$

over the finite field $R/\mathcal{P}$ with $\alpha \neq 0$. Hence, we get $N(\alpha) > 0$ and

$$\gamma_1 = \gamma(k, \mathcal{P}) \leq s \qquad \text{if } |G^k| \geq q^{\frac{1}{2}+\frac{1}{2s}}.$$

In particular, since $q \geq p \geq 3$, if $(k_1, q-1) \leq \frac{2}{3}q^{1/4}$ then we get $|G^k| \geq q^{3/4}$, hence $\gamma_1 \leq s = 2$. Also, if $(k_1, q-1) \leq \frac{2}{3}q^{1/3}$ then $|G^k| \geq q^{2/3}$, therefore $\gamma_1 \leq 3$. The second and third inequalities follow from the equation (4.9).

Finally, if $(k_1, q-1) \leq \frac{2}{3}q^{1/2}$ then $|G^k| \geq q^{1/2}$, and in this case Cipra [11], and independently Glibichuk [16], proved that $\gamma_1 \leq 8$. This, and the equation (4.9) yield the last inequality.

□

Notice that the method used in this section is very similar to that used in the proof of Theorem 3.6.1 and to obtain the upper bounds in Corollary 3.6.1. The key difference is that in this section we pay more attention to the set $\mathcal{A}$ and it's cardinality, where $\mathcal{A}$ is the subring consisting of sums of k-th powers in the residue ring $R_{\mathcal{P}}/(\pi^m)$. In the proof of Theorem 3.6.1 we only made use of the fact that $|\mathcal{A}| \leq q^n = p^{nf}$, whereas here we notice that $|\mathcal{A}| \leq p^{r\phi(t)}$, which leads us to the question, if t is the number of k-th power units in $R_{\mathcal{P}}/\mathcal{P}_{\mathcal{P}}{}^n$, and f is the degree of inertia of the prime ideal $\mathcal{P}$, then how do $\phi(t)$ and f compare? In other words which of the bounds is sharper? We would be able to answer those questions and obtain sharper bounds for Waring's number over algebraic number fields if we had sharper upper bounds and lower bounds for the cardinality of $\mathcal{A}$.

4.4 The Unramified Case

As before, in this section we let R be the ring of integers in a number field F. Let $\mathcal{P}$ be an *unramified* prime ideal in R, such that $\mathcal{P}$ lies over the odd rational prime p and has degree of inertia $f \geq 1$. Thus $\mathcal{P}\|(p)$. Let k be a positive integer, such that $k = p^r k_1$, and so $\mathcal{P}^r\|(k)$. Assume that $k_1|(q-1)$ where $q = p^f$ and set $t = (q-1)/k_1$. Recall that Theorem 4.3.2 implies that when $e = f = 1$ the problem is reduced to one discussed in Chapter 2 and we obtain the results in Theorems 2.3.1, 2.3.2 or 2.3.4. This section focuses on $f \geq 2$. We will prove the following main result

Theorem 4.4.1. *Let R be the ring of integers in a number field F. Let $\mathcal{P}$ be a prime ideal in R, such that $\mathcal{P}$ lies over the rational prime p and has degree of inertia $f \geq 2$. Let k be a positive integer, such that $k = p^r k_1$. Assume that $k_1|(q-1)$ where $q = p^f$ and set $t = (q-1)/k_1$. Also assume that the $\mathcal{P}$ is unramified, and that every element in the finite field $R/\mathcal{P} \cong R_{\mathcal{P}}/\mathcal{P}_{\mathcal{P}} = \mathbb{F}_q$ of q elements is expressible as a sum of k-th powers. Let*

$\gamma_1 = \gamma(k, \mathcal{P})$, *then for any positive integer* m,

$$\gamma(k, \mathcal{P}^m) \leq 2k \qquad \text{if } p = 2,$$

and if p *is odd*

$$\gamma(k, \mathcal{P}^m) \leq \begin{cases} \min\left\{\left(\frac{p}{p-1}\right)k + \delta, \frac{17}{2}\left(\frac{k}{k_1}\right)^{2.84/\log p} + \frac{1}{2}\right\} & \text{if } f \geq 2 \text{ and } k_1 \leq p^{f/2} \\ \min\left\{\left(\frac{p}{p-1}\right)k + \delta, \left(\frac{f}{p^{f/2-1}}\right)k\right\} & \text{if } f > 2 \text{ and } k_1 > p^{f/2} \\ \left(\frac{p}{p-1}\right)k + \delta & \text{if } f = 2 \text{ and } k_1 > p^{f/2} \end{cases}$$

where $\delta = 1$ *if* $k_1 = p - 1$ *and* $\delta = 0$ *otherwise.*

The proof of Theorem 4.4.1 follows immediately form Proposition 4.4.2 and Ramanujam's result [24, Proposition 1] which we give below in Proposition 4.4.1.

Suppose that the set of k-th powers in $R_{\mathcal{P}}/\mathcal{P}_{\mathcal{P}} = \mathbb{F}_{p^f}$ generates a subfield $\mathbb{F}_{q_1}$ with $q_1 = p^{f_1}$ elements where $f_1 | f$. Notice that here f_1 may be equal to f. Ramanujam proved in [24] (as shown in Lemmas 3.2.3 and 3.2.4) that if $\mathcal{A}_{k_1}$ is the subring of $R_{\mathcal{P}}$ generated by sums of k_1-th powers, then the subring

$$\mathfrak{N} = \left\{(x_0^{p^r} + px_1^{p^{r-1}} + \cdots + p^r x_r) \in R_{\mathcal{P}} \mid x_i \in \mathcal{A}_{k_1} \text{ for } i = 0, 1, \ldots, r\right\}$$

contains $\mathcal{A}_k$ which is the sub ring generated by sums of k-th powers in $R_{\mathcal{P}}$. Actually Ramanujam showed that the two set are equal unless $p = 2$ and $f_1 \neq f$.

Proposition 4.4.1. *[24, Ramanujam, Proposition 1] Let* R *be the ring of integers in a number field* F. *Let* $\mathcal{P}$ *be an prime ideal in* R, *such that* $\mathcal{P}$ *lies over the rational prime* p *and has degree of inertia* $f \geq 1$. *Let* k *be a positive integer, such that* $k = p^r k_1$ *with* $r \geq 1$ *and* $p \nmid k_1$. *Assume that* $k_1 | (q-1)$ *where* $q = p^f$. *Also, assume that* $\mathcal{P}$ *does not ramify. For any positive integer* m

$$\gamma(k, \mathcal{P}^m) \leq \left(\frac{p}{p-1}\right)k + \delta,$$

where $\delta = 1$ *if* $k_1 = p - 1$ *and* $\delta = 0$ *otherwise.*

To get the remaining upper bounds in Theorem 4.4.1, we have the following.

Proposition 4.4.2. *Let R be the ring of integers in a number field F. Let $\mathcal{P}$ be a prime ideal in R such that $\mathcal{P}$ lies over the odd rational prime p and has degree of inertia $f \geq 1$. Let k be a positive integer, such that $k = p^r k_1$. Assume that $k_1 | (q-1)$ where $q = p^f$ and set $t = (q-1)/k_1$. Also assume that the $\mathcal{P}$ is unramified, and that every element in the finite field $R/\mathcal{P} \cong R_{\mathcal{P}}/\mathcal{P}_{\mathcal{P}} = \mathbb{F}_q$ of q elements is expressible as a sum of k-th powers. Then for any positive integer m*

$$\gamma(k, \mathcal{P}^m) \leq \begin{cases} \frac{17}{2}\left(\frac{k}{k_1}\right)^{2.84/\log p} + \frac{1}{2} & \text{if } f \geq 2, \text{ and } k_1 \leq p^{f/2}, \\ \left(\frac{f}{p^{f/2-1}}\right) k & \text{if } f > 2, \text{ and } k_1 > p^{f/2}, \\ 2k & \text{if } f = 2, \text{ and } k_1 > p. \end{cases}$$

Lemma 4.4.1. *With the same assumptions as in Theorem 4.4.2, for any positive integer m we have*

$$\gamma(k, \mathcal{P}^m) \leq f\gamma(k, p^{r+1}),$$

where $\gamma(k, p^{r+1})$ is as defined in Chapter 2.

Proof. Since $\mathcal{P}$ does not ramify, and $p \geq 3$, by Theorem 3.2.1, we need only consider congruences modulo $\mathcal{P}^{n+1}$, where $n = er = r$. Also, it follows from Lemma 3.4.2 that the set of sums of k-th powers in $R/\mathcal{P}$ is spanned over $\mathbb{F}_p$ by the set of k-th power units $\mathcal{V} = \left\{\overline{1}, \overline{T}, \overline{T}^2, \ldots, \overline{T}^{\phi(t)-1}\right\}$. Here $T \in R$ is as in Section 3.4, that is, $T = a^k$ where a is a representative for the residue class which is a generator of the group of units in $R/\mathcal{P}$. Recall also that $\overline{T}$ is a primitive t-th root of unity in $R/\mathcal{P}^{r+1}$.

Furthermore, since every element in the finite field $R/\mathcal{P} \cong \mathbb{F}_q$ is expressible as a sum of k-th powers, there must be a set of f linearly independent (over $\mathbb{F}_p$) elements in the set $\mathcal{V}$, say $\left\{\overline{T}_1, \overline{T}_2, \ldots, \overline{T}_f\right\}$. In particular, $f \leq \phi(t)$.

Now, since $T_1, T_2, \ldots, T_f$ are elements is R such that $\overline{T}_1, \overline{T}_2, \ldots, \overline{T}_f \in R/\mathcal{P} = \mathbb{F}_{p^f}$ are linearly independent over $\mathbb{F}_p$, then as shown in Lemma 3.4.4 in Section 3.4, $T_1, T_2, \ldots, T_f$

are linearly independent over $\mathbb{Z}$ when viewed in $R/\mathcal{P}^{r+1}$. Consider the set

$$\mathcal{S} = \left\{ \sum_{i=1}^{f} n_i T_i \pmod{\mathcal{P}^{r+1}} \quad \middle| \quad 0 \leq n_i \leq p^{r+1} - 1 \right\}.$$

Then any two elements in S are distinct and

$$|\mathcal{S}| = \left| R/\mathcal{P}^{r+1} \right| = p^{(r+1)f}.$$

Therefore $\mathcal{S} = R/\mathcal{P}^{r+1}$.

For any element $\alpha \in R_k$, there exist rational integers $n_1, n_2, \ldots, n_f \in \mathbb{Z}/p^{r+1}\mathbb{Z}$ such that α can be represented as follows

$$\alpha \equiv \sum_{i=1}^{f} n_i T_i \pmod{\mathcal{P}^{r+1}}.$$

Let $s = \gamma(k, p^{r+1})$ be as defined in Chapter 2. Then there exist rational integers $x_{i1}, x_{i2}, \ldots, x_{is}$ such that

$$n_i = \sum_{j=1}^{s} x_{ij}^k + \lambda_i p^{r+1},$$

for some $\lambda_i \in \mathbb{Z}$, and thus

$$\alpha \equiv \sum_{i=1}^{f} \sum_{j=1}^{s} x_{ij}^k T_i \pmod{\mathcal{P}^{r+1}}.$$

Hence

$$\gamma(k, \mathcal{P}^m) \leq fs = f\gamma(k, p^{r+1}).$$

□

Remark:

Since $f \leq \phi(t)$, the upper bound in this result is sharper than the one obtained in Theorem 4.3.1.

Proof of Proposition 4.4.2. As in the proof of Lemma 4.4.1, since $\mathcal{P}$ does not ramify, and $p \geq 3$, by Theorem 3.2.1, we need only consider congruences modulo $\mathcal{P}^{r+1}$. If $k_1 \leq p^{f/2}$ then

$$t = \frac{p^f - 1}{k_1} \geq \frac{p^f - 1}{p^{f/2}} = p^{f/2} - \frac{1}{p^{f/2}},$$

and since $t \in \mathbb{Z}$ the last inequality implies that $t \geq p^{f/2}$. In this case Cipra [11] and independently Glibichuk [16], proved that

$$\gamma_1 = \gamma(k, \mathcal{P}) \leq 8.$$

Applying the lifting results in Corollary 3.2.1 (or equivalently Corollary 3.2.2), as in section 4.3, we get

$$\gamma(k, \mathcal{P}^{r+1}) \leq \frac{1}{2}\left[(2\gamma(k, \mathcal{P}) + 1)^{r+1} + 1\right].$$

That is, we get

$$\gamma(k, \mathcal{P}^{n+1}) \leq \frac{17}{2}(17)^r + \frac{1}{2}.$$

Since $k = k_1 p^r$ then $r = \log\left(\frac{k}{k_1}\right) / \log p$. Thus we obtain

$$\begin{aligned} \gamma(k, \mathcal{P}^{n+1}) &\leq \frac{17}{2}(17)^{\log\left(\frac{k}{k_1}\right)/\log p} + \frac{1}{2} \\ &\leq \frac{17}{2}\left(\frac{k}{k_1}\right)^{\log(17)/\log p} + \frac{1}{2} = \frac{17}{2}\left(\frac{k}{k_1}\right)^{2.84/\log p} + \frac{1}{2}. \end{aligned}$$

On the other hand, if $k_1 > p^{f/2}$ then from Lemma 4.4.1 we have

$$\begin{aligned} \gamma(k, \mathcal{P}^{r+1}) \leq f\gamma(k, p^{r+1}) &\leq fp^{r+1} \\ &= fp\frac{k}{k_1} \\ &< \left(\frac{fp}{p^{f/2}}\right)k = \left(\frac{f}{p^{f/2-1}}\right)k. \end{aligned}$$

Finally, we consider the case when $f = 2$ and $k_1 > p^{f/2} = p$. Then from Lemma 4.4.1 as above

$$\gamma(k, \mathcal{P}^{r+1}) \leq 2\gamma(k, p^{r+1}) \leq \frac{2kp}{k_1} < 2k.$$

□

Bibliography

[1] P. T. Bateman and R. M. Stemmler, W*aring's problem for algebraic number fields and primes of the form* $(p^r - 1)/(p^d - 1)$, Illinois J. Math **6** (1962), 142–156.

[2] N.F. Benschop, *Powersums representing residues mod* p^k*, from* F*ermat to* W*aring*, arXiv:math.BM/0103083 **2** (2001), 1–9.

[3] M. Bhaskaran, *Sums of m-th powers in algebraic and abelian number fields*, Archiv der Mathematik **17** (1966), 497–504.

[4] ———, *Sums of p-th powers in a p-adic ring*, Acta Arith. **15** (1969), 217–219.

[5] B. J. Birch, W*aring's problem in algebraic number fields*, Proc Cambridge Phil. Soc **57** (1961), 449–459.

[6] ———, W*aring's problem for* $\mathfrak{p}$*-adic number fields*, Acta Arith. **IX** (1964), 169–176.

[7] J.D. Bovey, *A note on* W*aring's problem in p-adic fields*, Acta Arith. **29** (1976), 343–351.

[8] ———, *A new upper bound for* W*aring's problem (mod p)*, Acta Arith. **32** (1977), 157–162.

[9] A. Cauchy, R*echerches sur les nombres*, J. Ecole Polytechnique **9** (1813), 99–116.

[10] I. Chowla, *On* W*aring's problem (mod p)*, Proc. Indian Nat. Acad. Sci. **13** (1943), 195–220.

[11] J. A. Cipra, W*aring's number in a finite field*, Integers **9** (2009), 435–440.

[12] ———, W*aring's problem in a finite field*, Kansas State University, Thesis (2009).

[13] T. Cochrane and J. Cipra, *Sum-product estimates applied to* W*aring's problem over finite fields*, preprint (2008).

[14] T. Cochrane and C. Pinner, *Sum-product estimates applied to* W*aring's problem (mod p)*, Integers **8** (2008).

[15] M.M. Dodson, *On* W*aring's problem in p-adic fields*, Acta Arith. **22** (1973), 315–327.

[16] A.A. Glibichuk, *Combinational properties of sets of residues modulo a prime and the* E*rdös-*G*raham problem*, Mat. Zametki, Translated in Math. Notes **79** (2006), 356–365.

[17] G.H. Hardy and J.E. Littlewood, *Some problems of "*P*artitio* N*umerorum", iv: The singular series in* W*aring's problem and the value of the number* $g(k)$, Math. Zeitshrift **12** (1922), 161–188.

[18] H. Heilbronn, *Lecture notes on additive number theory mod p*, California Institute of Technology (1964).

[19] D. Hilbert, B*eweis für die* D*arstellbarkeit der ganzen* Z*ahlen durch eine feste* A*nzahl* n^{ter} P*otenzen (*W*aringsches problem)*, Math. Ann. **67** (1909), 281300.

[20] L.K. Hua and H.S. Vandiver, *Characters over certain types of rings with applications to the theory of equations in a finite field*, Proc. Nat. Acad. Sci. U.S.A **25** (1949), 94–99.

[21] T. Cochrane J. A. Cipra and C. Pinner, H*eilbronn's conjecture on* W*aring's number (mod p)*, J. Number Theory **125** (2007), 289–297.

[22] S.V. Konyagin, *On estimates of* G*aussian sums and* W*aring's problem for a prime modulus*, Trudy Mat. Inst. Stelov.(Russian),Proc. Steklov Inst. Math. (English trans.) **198, 1** (1992, 1994), 11–124, 105–117.

[23] E. Landau, *Über einige* F*ortschritte der* A*dditiven* Z*ahlentheorie*, Cambridge Univ. Press (1937).

[24] C. P. Ramanujam, *Sums of m-th powers in p-adic rings*, Mathematika **10** (1963), 137–146.

[25] H.B. Mann S. Chowla and E.G. Straus, *Some applications of the* C*auchy*-D*avenport theorem*, Norske Vid. Selsk. Forh. Trondheim **32** (1959), 74–80.

[26] C. Siegel, *Additive theorie der zahlkörper. i*, Math. Ann. **87** (1922), 1–35.

[27] ———, *Generalization of* W*aring's problem to algebraic number fields.*, American Journal of Mathematics **66** (1944), 122–136.

[28] C. Small, *Solution of* W*aring's problem mod n*, American Math. Monthly **84** (1977), 356–359.

[29] ———, W*aring's problem mod n*, American Math. Monthly **84** (1977), 12–25.

[30] R. M. Stemmler, *The easier* W*aring's problem in algebraic number fields*, Acta Arith. **VI** (1961), 447–468.

[31] J. Subocz, *A note on* W*aring's number modulo* 2^n, Divulg. Mat. **7** (1999), 13–18.

[32] L. Tornheim, *Sums of n-th powers in fields of prime characteristic*, Duke Math J. **4** (1938), 395–362.

[33] R. C. Vaughan and T. D. Wooley, W*aring's problem: A survey*, Book: Number Theory for the Millenium **III** (2002), 301–340.

[34] J.F. Voloch, *On the p-adic* W*aring's problem*, Acta Arith. **90** (1999), 91–95.

[35] A. Weil, *Number of solutions of equations in finite fields*, Bull. AMS **55** (1949), 497–508.

[36] A. Winterhof, *On* W*aring's problem in finite fields*, Acta Arith. **87** (1998), 171–177.

[37] ———, *A note on* W*aring's problem in finite fields*, Acta Arith. **96** (2001), 365–368.

Appendix A

UBASIC Program

The UBASIC Program used to extend the range for p in the result obtained by Voloch [34] that $\gamma(p, p^2) \leq 3$ for $p \leq 211$ except for $p = 3, 7, 11, 17$ and 59 to $p \leq 1000$.

10 dim $C\%(10000)$:dim $P\%(10000)$:dim $M\%(10000)$

20 input P

30 for $I = 0$ to P

40 $M\%(I) = 0$:next I

50 $P2 = P^2$

60 for $A = 1$ to $P - 1$

70 for $D = 1$ to $(P - 1) \setminus 2$

80 if $(p - 1)@D = 0$ then goto 100

90 next D

100 if modpow$(A, D, P) = 1$ then cancel for:next A

110 next D

130 if modpow$(A, P - 1, P2) = 1$then $A = A + P$

135 print "$a =$ ";A

140 for $I = 0$ to $P - 1$

150 $C\%(I)$ =modpow$(A, I, P2)$

170 next I

180 for $J = 0$ to $P - 1$

190 $P\%(J)$ =modpow$(J, P, P2)$

200 next J

210 for $B = 0$ to $P - 1$:for $C = 0$ to B

220 $S = (1 + P\%(B) + P\%(C))@P2$

230 $S1$ =movinv$(S, P2)$

240 for $K = 1$ to $P - 1$

250 if modpow$(C\%(K) * S1, P - 1, P2) = 1$ then $M\%(K) = 1$

260 next K

270 next C:next B

280 for $I = 0$ to $P - 1$

290 if $M\%(I) = 0$ then print "Exception",P,$C\%(I)$

300 next I

310 P=nxtprm(P)

315 print "$p =$ ";P

320 goto 30