Primitive roots in algebraic number fields

Research Thesis

Submitted in partial fulfillment of the requirements

for the Degree of Doctor of Philosophy

Joseph Cohen

Submitted to the Senate of
the Technion — Israel Institute of Technology
Elul 5764 Haifa September 2004

The research was carried out in the Faculty of Mathematics under supervision of Professor Jack Sonn and Professor Zeev Rudnick .

The generous financial help of the Technion is gratefully acknowledged.

Contents

Abstract

We consider an analogue of Artin's primitive root conjecture for units in real quadratic fields. Given such a nontrivial unit, for a rational prime p which is inert in the field. The maximal order of this unit modulo p is $p+1$. An extension of Artin's conjecture is that there are infinitely many such inert primes for which this order is maximal. This is known at present only under the Generalized Riemann Hypothesis. Unconditionally, we show that for any choice of 7 units in different real quadratic fields satisfying a certain simple restriction, there is at least one which satisfies the above version of Artin's conjecture. Likewise, we consider an analogue of Artin's primitive root conjecture for nonunits in real quadratic fields. Given such an element, for a rational prime p which is inert in the field the maximal order of the unit modulo p is p^2-1. As before, the extension of Artin's conjecture is that there are infinitely many such inert primes for which this order is maximal. We show that out of any choice of 85 algebraic numbers satisfying a certain simple restriction, there is at least one which satisfies the above version of Artin's conjecture.

Gupta and Murty's method to attack the former problems raises question regarding $\gcd(a^n-1, b^n-1)$ where a, b are multiplicatively independent rational positive integers. It is known that there are infinitely many integers n with ’big‘ $\gcd(a^n-1, b^n-1)$. We show the same property for $\gcd(a^n+1, b^n+1)$.

By the principal method which we use for primitive roots we can obtain another result. Let $\ell_r(p)$ ($\ell_{nr}(p)$ respectively) denote the smallest prime which is quadratic residue (non-residue respectively) *mod* p, and $z(x)$ any unbounded increasing real function. We show the known results of Erdös and Elliot with an elementary method, and generalize this result in the sense that the $\ell_r(p)$'s ($\ell_{nr}(p)$'s) can be chosen from a specific infinite set which fulfills a certain condition . Then, we present an interesting application of the proof technique of the result which relates to the former problem.

1. Abbreviations and Notations

$\mathbb{Z}$ - The ring of integers.

$\mathbb{Z}/p$ - The ring of integers modulo prime p

$\mathbb{F}_p^\star$ - Multiplicative group of the field of p elements

$< a >$ - Subgroup of $\mathbb{F}_p^\star$ which generate by a

$gcd(,)$ - Greatest common divisor of two integers

$\mathrm{ord}(q)$ - Order of element in $\mathbb{F}_p^\star$

$(\frac{q}{p})$ - Legendre symbol

$\Omega(n)$ - Number of prime factors of n (with multiplicity)

$f \ll g$ (or $g \gg f$ or $f = O(g))$) - The inequality $|f(x)| \leq cg(x)$.

$f(x) = o(g(x))$ - Means that $\frac{f(x)}{g(x)} \to 0$

Δ - The discriminant of the real quadratic field

$K = \mathbb{Q}(\sqrt{\Delta})$ - A real quadratic field

$\mathcal{O}_K$ - Integer ring of K

$\Pi(y; m, s)$ - Number of primes $p \leq y$ such that $p \equiv s \ (mod\ m)$

$Li(y)$ - The term $\int_2^y \frac{dt}{\log t}$

$E(y; m, s)$ - The term $\Pi(y; m, s)$ -$\frac{Li(y)}{\varphi(m)}$

$E(x, m) = \max\limits_{1 \leq y \leq x} \max\limits_{(s,m)=1} |E(y; m, s)|$

$\varphi(m)$ - Euler totient

$C_\epsilon(p)$ -Kernel of a map $(\mathcal{O}_K/(p))^* \mapsto (\mathbb{Z}/p)^*$

$\mathcal{N}$ - The norm map

ν - Function which gives, the number of prime factors of an integer

μ - Möbius function

$S(\mathcal{A}, z, v) - |\{a | a \in \mathcal{A}, (a, \prod\limits_{p<z,\ p\nmid v} p) = 1\}|$

$ord(A, N)$ - Order of the matrix $A \ mod\ N$.

$ord(a, b; N)$ - Order of $(a, b) \ mod\ N$

$P_a(z)$ - The product of all odd primes up to z and $\equiv a(mod\ 4)$

$P(z) = P_1(z)P_3(z)$.

P_3 - Integer with at most three prime divisors

$\ell_r(p)$ $(\ell_{nr}(p))$ - The smallest prime which is a quadratic
residue (non-residue) $mod\ p$

2. Introduction

A natural question to ask is if there are many primes for which 2 is a primitive root, that is if the subgroup $\langle 2 \rangle$ of the multiplicative group $\mathbb{F}_p^\star$ of the field of p elements generated by 2 is the whole group. Is there a finite number of such groups $\mathbb{F}_p^\star$? Does the same apply for any integer a?

In 1927 Emil Artin [2] made the following conjecture:

Conjecture 2.1. *Let $a \neq -1$ be an integer which is not a perfect square. Then there are infinitely many primes p such that*

$$< a >= \mathbb{F}_p^\star \ .$$

In addition, for $x > 0$, the number of primes $p \leq x$ with this property is asymptotic as $x \to \infty$ to

$$A(a) \frac{x}{\log x}$$

where $A(a)$ is a constant which depends on a.

In 1967 Hooley [13] proved Artin's conjecture with the asymptotic formula under the Generalized Riemann Hypothesis. In 1983 Gupta and Murty [9] proved that there are 13 specific integers such that at least one of them fulfills the Artin conjecture. From the proof we can deduce that Artin's conjecture is true for almost all integers. R. Murty, K. Murty and Gupta [10] showed that we can reduce the specific set of integers from 13 to 7. Improving the analytic part of Gupta and Murty enabled to give the best result till now:

Theorem 2.2. ([12]) *Let q, r and s any three primes. Then at least one of them is a primitive root mod p for infinitely many primes p.*

We note that theorem 5.1 holds for any three non-zero integers, q, r and s which are multiplicatively independent where q, r, s, $-3qr$, $-3qs$, $-3rs$ and qrs are not a square. (we say that r integers $a_1, ..., a_r$ are multiplicatively independent if for any integers $n_1, ..., n_r$, $a_1^{n_1} \cdots a_r^{n_r} = 1 \Rightarrow n_1 = ... = n_r = 0$).

In this work we present an analog of Artin's conjecture in a quadratic field and we will prove a result similar to the one just shown (we will show that a set which contains a specific number of elements or more always contains a primitive root) for units (in chapter 2) and for any algebraic number which is not unit (in chapter 3).

Another interesting problem which was raised from the Gupta and Murty work is to find an infinite sequence of integers n such that $gcd(a^n - 1, b^n - 1) = 1$. Ailon and Rudnick [1] have conjectured that the answer is true. From this, a natural question to ask is if there exists an infinite sequence of integers n such that the $gcd(a^n - 1, b^n - 1)$ is big. Let a, b be multiplicatively independent. Y. Bugeaud, P. Corvaja and U. Zannier [4] proved that for all $\epsilon > 0$, $gcd(a^n - 1, b^n - 1) < c(\epsilon)exp(\epsilon n)$. L. Adleman, C. Pomerance and R. Rumely [3] proved that there are infinitely many integers n such that $gcd(a^n - 1, b^n - 1) > exp(exp(c \log n / \log\log n))$ for any integers a, b.

In chapter 6 we prove the same result as APR found result for $gcd(a^n + 1, b^n + 1)$. In addition we note that this is also true for $gcd(a^n + 1, b^n - 1)$.

In the last chapter we show an interesting use by elementary sieve method (the method which we use for the primitive roots result) to solve two problems from number theory one of them related to the above mentioned problem.

3. The work of Gupta-Murty and of Heath-Brown

Since our work is based on the idea of Gupta and Murty with the advanced version as in the paper of Heath-Brown it will be natural to present their work. We start with following trivial idea: since the number of elements in $\mathbb{F}_p^\star$ is $p - 1$, if we show for all integer d, and infinitely many primes p

$$d \mid p - 1, d \neq p - 1 \Rightarrow a^d \not\equiv 1 \ \ mod\ p$$

we will have proven the conjecture.

So our first goal is to find infinitely many primes p with a small number of prime divisors of $p - 1$. Heath-Brown proved the following lemma.

Lemma 3.1. *Let q, r and s be any three primes. There exist $K = 2^k$, $k = 1, 2, 3$ such that for any sufficiently large $x \in \mathbb{R}^+$ we have two numbers $\epsilon, \delta \in (0, 1/4)$ and $c = c(\epsilon, \delta) > 0$ so that there are at least $c\frac{x}{\log^2 x}$ primes $p \le x$ which satisfy:*

Either $\frac{p-1}{K}$ is prime or $\frac{p-1}{K} = p_1 p_2$ for p_1, p_2 primes $> p^{1/4+\epsilon}$ and $p_1 < p^{1/2-\delta}$. Furthermore, p satisfies

$$(\frac{q}{p}) = (\frac{r}{p}) = (\frac{s}{p}) = -1.$$

Now we prove theorem 5.1 from this lemma. Assume for simplicity that $K = 2$ and that we have infinitely many primes $p \le x$ as in the Lemma 3.1 such that $\frac{p-1}{2} = l$ where l is a prime. Take one of the three primes in the lemma, say, q. If the order of q equals l we get a contradiction to the fact that $(\frac{q}{p}) = -1$ by the theorem on cyclic groups (the order of the squares subgroup of $\mathbb{F}_p^\star$ is $\frac{p-1}{2} = l$). If $\mathrm{ord}(q) = 2l$ we are done. If not, the only possibility left is $\mathrm{ord}(q) = 2$ but this does not occur for sufficiently large primes p and hence q is a primitive root.

Assume now that there exist $c\frac{x}{\log^2 x}$ primes $p \le x$ as in Lemma 3.1 such that $\frac{p-1}{2} = p_1 p_2$. As before the order of q, r and s can be (if they are not primitive) 2, $2p_1$ or $2p_2$. As before there is only a small number of cases where $\mathrm{ord}(q) = 2$. Assume that $\mathrm{ord}(q) = 2p_1$. For this case we need some observation. Let n be a natural number and $\Omega(n)$ denote the number of prime factors of n (with multiplicity) and write $f \ll g$ (or $g \gg f$ or $f = O(g)$), where g is a positive function, if there exists a constant $c > 0$ such that $|f(x)| \le cg(x)$. Then

Observation 3.2. *(1) For any natural number n, $\Omega(n) \ll \log n$.*

(2) Given an integer a, The number of primes p such that $\mathrm{ord}(a) < y$ *(mod p) is $O(y^2)$.*

To see (1), use $n = q_1^{\alpha_1} \cdots q_r^{\alpha_r} \ge 2^{\alpha_1} \cdots 2^{\alpha_r} \ge 2^{\alpha_1 + \ldots + \alpha_r} = 2^{\Omega(n)}$. To see (2), use $\sum\limits_{m<y} \Omega(a^m - 1) \ll_a \sum\limits_{m<y} \log(a^m - 1) \ll_a \sum\limits_{m<y} m \ll_a y^2$.

Now, if $\mathrm{ord}(q) = 2p_1 < x^{1/2-\delta}$ *(mod p)*, then by observation 3.2 this occurs for at most $(x^{1/2-\delta})^2 = x^{1-2\delta}$ primes.

Since $\frac{x^{1-2\delta}}{cx/\log^2 x} \to 0$ as $x \to \infty$ there are a negligible number of primes p such that $\mathrm{ord}(q) = 2p_1$ *(mod p)*. This fact is also true for r and s.

Now, assume that q and r and s have order $2p_2$. Since $\mathbb{F}_p^\star$ is a cyclic group, $\mathrm{ord}(< q, r, s >) = 2p_2 < x^{3/4-\epsilon}$. By Lemma 2 in [9] the number of primes p such that $\mathrm{ord}(< q, r, s >) < y$ is $O(y^{4/3})$. So the number of primes p such that $\mathrm{ord}(< q, r, s >) = 2p_2 < x^{3/4-\epsilon}$ is $O(x^{1-4\epsilon/3})$ and as before, is negligible in comparison to $\frac{cx}{\log^2 x}$.

4. Artin's conjecture in a real quadratic field for units

Let $d \neq 1$ be a square-free natural number and let $\Delta = d$ if $d \equiv 1(mod\ 4)$ and $\Delta = 4d$ otherwise. Let $K = \mathbb{Q}(\sqrt{\Delta})$ be a real quadratic field and denote the integer ring of K by $\mathcal{O}_K$. The principal ideals $p\mathcal{O}_K$ that are generated by a rational prime p, take one of the following forms

(1) $p\mathcal{O}_K = P$ (inert);
(2) $p\mathcal{O}_K = P_1P_2, \quad P_1 \neq P_2$ (splits);
(3) $p\mathcal{O}_K = P^2$ (ramified)

where P and P_i are prime ideals in $\mathcal{O}_K$. We note that the option (3) occurs only in a finite number of cases and so does not interest us.

Now, the norm map

$$\mathcal{N} : \mathcal{O}_K \mapsto \mathbb{Z}$$

gives a homomorphism

$$(O_K/(p))^* \mapsto (\mathbb{Z}/p)^*$$

For any unit ϵ with $\mathcal{N}(\epsilon) = 1$ the kernel of this map contains the residue class ϵ modulo p. Denote this kernel by $C_\epsilon(p)$. By Lemma 19 in [15] (appendix B)

$$\mathrm{ord}(C_\epsilon(p)) = \begin{cases} p-1, & p\ splits \\ p+1, & p\ inert \end{cases}$$

Assuming GRH, Cooke and Weinberger ([8]) and Lenstra ([16]) showed that given a real quadratic field K, there are infinitely many split primes for which the fundamental unit of the field has maximal order (namely $p-1$) in $C_\epsilon(p)$.

Using the strong analytic theorem of Heath-Brown [13], Narkiewicz [19] proved the following unconditional theorem:

Theorem 4.1. *Let $\epsilon_1, \epsilon_2, \epsilon_3$ be units in the integer rings $\mathcal{O}_{K_1}, \mathcal{O}_{K_2}, \mathcal{O}_{K_3}$ of $K_1 = \mathbb{Q}(\sqrt{\Delta_1})$, $K_2 = \mathbb{Q}(\sqrt{\Delta_2})$, $K_3 = \mathbb{Q}(\sqrt{\Delta_3})$, respectively, which* *are not roots of unity. There is an index j, $1 \leq j \leq 3$, such that for infinitely many split primes p, $c_j\epsilon_j$, $c_j = \pm 1$, has order $p-1$ (mod (p)).*

For inert primes, one wants similar results. Under GRH, an analogue of [8] [16] was only proven recently by Roskam ([20]). We want to extend the result of Narkiewicz for inert primes. In this case the order of $C_\epsilon(p)$ $(mod\ p)$ is $p+1$. So we cannot use the result of Heath-Brown on the divisors of $p-1$. We shall use a simpler method to get infinitely many primes p such that $\frac{p+1}{2} = P_3$ (we write P_3 for an integer with at most three prime factors) but with almost same magnitude of the prime divisors. With this result we obtain:

Theorem 4.2. *Let $\epsilon_1, \ldots, \epsilon_7$ be units (assume that they have norm $+1$) in the rings of integers $\mathcal{O}_{\Delta_1}, \ldots, \mathcal{O}_{\Delta_7}$ of $\mathbb{Q}(\sqrt{\Delta_1}), \ldots, \mathbb{Q}(\sqrt{\Delta_7})$, respectively, which are not roots of unity, with $\Delta_1, \ldots, \Delta_7$ multiplicatively independent and distinct from 3. Assume that all the numbers $(-1)^{a_1} 3^{a_2} \prod_{i=1}^{7} \Delta_i^{b_i}$, $a_i, b_i \in \{0, 1\}$, are not perfect squares if $\sum_{i=1}^{7} b_i$ is odd. Then there exists an index $1 \leq j \leq 7$, such that for infinitely many inert primes p, the unit $c_j\epsilon_j$, $(c_j = \pm 1)$, has order $p+1$ modulo $p\mathcal{O}_{\Delta_j}$.*

Corollary 4.3. *Let $\epsilon_1, \ldots, \epsilon_7$ be units (assume that they have norm $+1$) in the rings of integers $\mathcal{O}_{\Delta_1}, \ldots, \mathcal{O}_{\Delta_7}$ of $\mathbb{Q}(\sqrt{\Delta_1}), \ldots, \mathbb{Q}(\sqrt{\Delta_7})$, respectively, which are not roots of unity, with $\Delta_1, \ldots, \Delta_7$ primes distinct from 3. Then there exists an index $1 \leq j \leq 7$, such that for infinitely many inert primes p, the unit $c_j\epsilon_j$, $(c_j = \pm 1)$ has order $p+1$ modulo $p\mathcal{O}_{\Delta_j}$.*

4.1. **Notation and Preliminaries.** Now before we prove the theorem about the prime divisors of $p+1$ (as in Lemma 3.1 for $p-1$) we need to decide on some notation.

Let $\Pi(y; m, s)$ denote the number of primes $p \leq x$ such that $p \equiv s$ $(mod\ m)$ where m and s are some integers, and

$$E(y; m, s) := \Pi(y; m, s) - \frac{Li(y)}{\varphi(m)}$$

where $Li(y) = \int_2^y \frac{dt}{\log t}$. Also set

$$E(x; m) := \max_{1 \leq y \leq x} \max_{(s,m)=1} |E(y; m, s)|\ .$$

Define $\mathcal{A} = \{p+1|p \leq x, p \equiv u \ (mod\ v)\}$ where $u,\ v$ are some integers such that $(u,v)=1,\ u \equiv 1(\mod 2),\ 8|v,\ (\frac{u+1}{2}, v) = 1$ and take $X = \frac{Li(x)}{\varphi(v)}$.

For a square-free integer d, $(d,v)=1$, let

$$\begin{aligned}\mathcal{A}_d &:= \{a \in \mathcal{A} : a \equiv 0 \mod d)\}\\ &= \{p+1 : p \leq x,\ p \equiv u \mod v,\ p \equiv -1 \mod d\}\end{aligned}$$

By the Chinese remainder theorem there exists an l such that

$$|\mathcal{A}_d| = \#\{p+1|p \leq x, p \equiv l\ (mod\ dv)\}\ .$$

By the definition of $E(x; dv, l)$,

$$|\mathcal{A}_d| = \frac{Lix}{\varphi(dv)} + E(x; dv, l) = \frac{1}{\varphi(d)}\frac{Lix}{\varphi(v)} + E(x; dv, l) = \frac{X}{\varphi(d)} + E(x; dv, l)$$

Define $\omega(d) := \frac{d}{\varphi(d)}$ and

$$R_d := |\mathcal{A}_d| - \frac{\omega(d)}{d}X = E(x; dv, l)$$

Finally, we define two arithmetical functions for a square-free $d = p_1 \cdot \cdot \cdot p_k$. $\mu(d) = (-1)^k$ and $\nu(d) = k$ (where $\mu(1) = 1$ and $\nu(1) = 0$).

Now we want to prove two lemmas.

Lemma 4.4. *For any prime q, which is relatively prime to v we have:*

$$0 \leq \frac{1}{q-1} \leq 1 - \frac{1}{c_1} \tag{4.1}$$

where $c_1 > 1$ is some suitable constant.

$$\sum_{w \leq q < z} \frac{\log q}{q-1} - \log\frac{z}{w} = O(1) \quad (2 \leq w \leq z) \tag{4.2}$$

where O does not depend on z or w.

$$\prod_{\substack{2<q<z\\ q\nmid v}} (1 - \frac{1}{q-1}) \gg \frac{1}{\log z}. \tag{4.3}$$

Proof. Since $q > 2$ it is clear that (7.3) holds.

As for the second equation, $\sum\limits_{w \leq q < z} \frac{\log q}{q-1} = \sum\limits_{w \leq q < z} \frac{\log q}{q} \frac{q}{q-1} = \sum\limits_{w \leq q < z} \frac{\log q}{q}(1 + \frac{1}{q-1}) = \sum\limits_{w \leq q < z} \frac{\log q}{q} + \sum\limits_{w \leq q < z} \frac{\log q}{q(q-1)} = \log \frac{z}{w} + O(1) \qquad (\sum\limits_{p < x} \frac{\log p}{p} = \log x + O(1))$.

Hence we get (7.4). Finally,

$$\begin{aligned}\prod_{\substack{2<q<z \\ q \nmid v}} (1 - \frac{\omega(q)}{q}) = \prod_{\substack{2<q<z \\ q \nmid v}} (1 - \frac{1}{q-1}) \gg \prod_{2<q<z} (1 - \frac{1}{q-1}) \\ = \exp(\log \prod_{2<q<z} (1 - \frac{1}{q-1})) \\ = \exp(\sum_{2<q<z} \log (1 - \frac{1}{q-1})) \\ \gg \exp(\sum_{2<q<z} (-\frac{1}{q-1} - \frac{1}{(q-1)^2}))\end{aligned}$$

Since

$$\frac{1}{q-1} = \frac{1}{q} + \frac{1}{q(q-1)} \leq \frac{1}{q} + \frac{1}{(q-1)^2}$$

and $\sum\limits_{2<q<z} \frac{1}{(q-1)^2}$ converges, we get

$$\prod_{2<q<z} (1 - \frac{1}{q-1}) \gg \exp(-\sum_{2<q<z} \frac{1}{q}).$$

Since

$$\sum_{2<q<z} \frac{1}{q} \sim \log \log z$$

we have

$$\exp(-\sum_{2<q<z} \frac{1}{q}) \gg \exp(-\log \log z) = \frac{1}{\log z}$$

□

Lemma 4.5. *For any natural square-free number d, $(d, v) = 1$, given an $A > 0$ there exist constants $c_2 (\geq 1)$ and $c_3 (\geq 1)$ such that*

$$\sum_{d < \frac{X^{\frac{1}{2}}}{(\log x)^{c_2}}} \mu^2(d) 3^{\nu(d)} |R_d| \leq c_3 \frac{X}{\log^A X}, \quad (X \geq 2) \tag{4.4}$$

Proof. Denote by S_{R_d} the term which we need to estimate:

$$S_{R_d} = \sum_{d<\frac{X^{\frac{1}{2}}}{(\log x)^{c_2}}} \mu^2(d)3^{\nu(d)}|R_d|.$$

By the definitions of R_d and $E(x;dv)$

$$S_{R_d} \leq \sum_{d<\frac{X^{\frac{1}{2}}}{(\log x)^{c_2}}} \mu^2(d)3^{\nu(d)}|E(x;dv)|.$$

Since $E(x;dv) \ll \frac{x}{dv}$ if $d \leq \frac{x}{v}$, we get that

$$S_{R_d} \ll \sum_{d<\frac{X^{\frac{1}{2}}}{(\log x)^{c_2}}} \mu^2(d)3^{\nu(d)}|E(x;dv)|^{\frac{1}{2}}(\frac{x}{dv})^{\frac{1}{2}}.$$

Hence,

$$S_{R_d} \ll x^{\frac{1}{2}} \sum_{d<\frac{X^{\frac{1}{2}}}{(\log x)^{c_2}}} \frac{\mu^2(d)3^{\nu(d)}}{d^{\frac{1}{2}}}|E(x;dv)|^{\frac{1}{2}}.$$

By Cauchy's inequality,

$$S_{R_d} \ll x^{\frac{1}{2}}(\sum_{d<\frac{X^{\frac{1}{2}}}{(\log x)^{c_2}}} \frac{\mu^2(d)3^{2\nu(d)}}{d})^{\frac{1}{2}}(\sum_{d<\frac{X^{\frac{1}{2}}}{(\log x)^{c_2}}} |E(x;dv)|)^{\frac{1}{2}}.$$

We have,

$$S_{R_d} \ll x^{\frac{1}{2}}(\sum_{d<X^{\frac{1}{2}}} \frac{\mu^2(d)3^{2\nu(d)}}{d})^{\frac{1}{2}}(\sum_{dv<\frac{vX^{\frac{1}{2}}}{(\log x)^{c_2}}} |E(x;dv)|)^{\frac{1}{2}}.$$

For sufficiently large x we obtain

$$S_{R_d} \ll x^{\frac{1}{2}}(\sum_{d<x^{\frac{1}{2}}} \frac{\mu^2(d)3^{2\nu(d)}}{d})^{\frac{1}{2}}(\sum_{dv<\frac{x^{\frac{1}{2}}}{(\log x)^{c_2}}} |E(x;dv)|)^{\frac{1}{2}}.$$

With Bombieri-Vinogradov theorem ([5]) (given any positive constant e_1, there exist a positive constant e_2 such that $\sum_{d<\frac{x^{\frac{1}{2}}}{\log^{e_2} x}} E(x;d) = O(\frac{x}{\log^{e_1} x})$) for the last sum and since $\sum_{d<w} \frac{\mu^2(d)9^{\nu(d)}}{d} \leq (\log w + 1)^9$ (see

[11], p.115, equation (6.7)) we find that for given constant B there exist c_2 such that

$$S_{R_d} \ll \frac{x}{\log^B x}$$

So, for given A there exist c_2 such that

$$S_{R_d} \ll \frac{X}{\log^A X}$$

where $\ll$ depends on v and c_2. □

4.2. **Proof of Theorem 4.2 - the sieve part.** In this section we will show that for a sufficiently small $0 < \delta < 1/4$ there exists some constant $c(\delta) > 0$ (which depends on δ) such that for at least $c(\delta)\frac{x}{\log^2 x}$ primes $p \leq x,\ p \equiv u\ (mod\ v),\ \frac{p+1}{2} = P_3$ where $q|\frac{p+1}{2} \Rightarrow q > x^{1/4-\delta}$. Later we will sharpen this result further.

4.2.1. *Use of the lower bound linear sieve.* In the following subsection we will show, using the linear sieve, that for a sufficiently small $0 < \delta < 1/4$ there exists some constant $c_1(\delta) > 0$ (which depends on δ) such that for at least $c_1(\delta)\frac{x}{\log^2 x}$ primes $p \leq x,\ p \equiv u\ (mod\ v),\ \frac{p+1}{2}$ has at most four prime divisors all of them greater than $x^{\frac{1}{4}-\delta}$.

Define $S(\mathcal{A}, z, v) = \#\{a | a \in \mathcal{A}, (a, \prod_{\substack{p<z \\ p\nmid v}} p) = 1\}$ and let f denote the "lower bound function" for the linear sieve which is defined as $f(t) = 2e^{\gamma}t^{-1}\log(t-1)$ for $2 \leq t \leq 4$, where γ is Euler constant. Then (see [11, Theorem 8.4, page 236]):

Lemma 4.6. *Assume* (7.3)*,* (7.4) *and* (5.4)*. Then for* $X^{1/8} < z < X^{1/4}$ *we have*

$$S(\mathcal{A}, z, v) \geq X \prod_{\substack{q<z \\ q\nmid v}} (1 - \frac{\omega(q)}{q})\{f(\frac{\log x}{2\log z}) + O(\frac{1}{\log x})\} \tag{4.5}$$

where the O-term does not depend on X or on z.

Note 4.7. Obviously z influences the number of primes which divide the elements of $\mathcal{A}$ and their magnitude. Heath-Brown used a stronger version of this lemma which gives $z = x^{1/4+\epsilon_0}$ where ϵ_0 is a specific small real number.

By Lemmas 5.3 and 4.5, (7.3), (7.4) and (5.4) hold. Hence we can use Lemma 5.5 with $z = X^{\frac{1}{4}-\delta}$.

$$S(\mathcal{A}, X^{\frac{1}{4}-\delta}, v) \geq X \prod_{\substack{q < X^{\frac{1}{4}-\delta} \\ q \nmid v}} (1 - \frac{1}{q-1})\{f(\frac{1}{2}\frac{\log x}{\log x^{\frac{1}{4}-\delta}}) + O(\frac{1}{\log x})\}.$$

By Lemma 5.3 (5.3) we have

$$S(\mathcal{A}, X^{\frac{1}{4}-\delta}, v) \gg \frac{X}{\log x^{\frac{1}{4}-\delta}} f(\frac{2}{1-4\delta}).$$

But for $2 \leq t \leq 4$, $f(t) = 2e^{\gamma}t^{-1}\log(t-1)$, and so,

$$\begin{aligned} S(\mathcal{A}, X^{\frac{1}{4}-\delta}, v) &\gg \frac{X}{\log x^{1/4-\delta}} 2e^{\gamma}(\frac{1-4\delta}{2}) \log \frac{1+4\delta}{1-4\delta} \\ &\gg \frac{x}{\log^2 x} \log \frac{1+4\delta}{1-4\delta} = \frac{x}{\log^2 x} \log(1 + \frac{8\delta}{1-4\delta}). \end{aligned}$$

Since $\log(1+s)/s \sim 1$ as $s \to 0$ and for, $0 < \delta < 1/4$, $1 - 4\delta$ are bounded, we have:

Lemma 4.8.

$$S(\mathcal{A}, X^{\frac{1}{4}-\delta}, v) \gg \delta \frac{x}{\log^2 x}$$

where the implied constant in $\gg$ does not depend on δ.

Note 4.9. By definition of $S(\mathcal{A}, X^{\frac{1}{4}-\delta}, v)$, for all sufficiently small $0 < \delta < 1/4$, there are $\gg \delta \frac{x}{\log^2 x}$ primes $p \leq x$, such that any prime divisor of $p+1$ (for a p in our sequence) is greater than $X^{\frac{1}{4}-\delta}$ or divides v. Since by our assumption $(\frac{u+1}{2}, v) = 1$ where $p \equiv u \ (mod\ v)$ and $X = \frac{Li(x)}{\varphi(v)}$ we obtain that all odd prime divisor of $\frac{p+1}{2}$ are greater than $x^{\frac{1}{4}-\delta}$. Hence there are at most four prime divisors of $\frac{p+1}{2}$ which are greater than $x^{\frac{1}{4}-\delta}$. In the next subsection we will show that there are only a small number of primes $p \leq x$ such that $\frac{p+1}{2}$ has exactly four prime divisors all of which are greater than $x^{\frac{1}{4}-\delta}$.

4.2.2. *First use of the Selberg upper bound sieve.* In order to prove that there are only a small number of primes $p \leq x$ such that exactly four primes divide $\frac{p+1}{2}$ we need to use Selberg's upper bound sieve (see [11, theorem 3.12]):

Proposition 4.10. *Let a, b be integers satisfying*

$$ab \neq 0, \quad \gcd(a,b) = 1, \quad 2 \mid ab$$

Then as $x \to \infty$ we have uniformly in a, b that

$$|\{p : p \leq x,\ ap + b = \text{ prime}\}| \leq$$
$$8 \prod_{p>2} (1 - \frac{1}{(p-1)^2}) \prod_{2<p|ab} \frac{p-1}{p-2} \frac{x}{\log^2 x} \{1 + O(\frac{\log\log x}{\log x})\}$$

From this proposition we derive the following:

Lemma 4.11. *For any $0 < \delta < 1/4$, there exists $c_2(\delta)\frac{x}{\log^2 x}$ $(c_2(\delta) > 0)$ primes $p \leq x$ such that $\frac{p+1}{2}$ has at most three prime divisors all of which are greater than $x^{1/4-\delta}$.*

Proof. Assume that $\frac{p+1}{2} = p_1p_2p_3p_4,\ p \leq x$ where the p_i are primes greater than $x^{1/4-\delta}$. Instead of counting the elements in this set we can count the products of primes $p_1p_2p_3p_4$ such that $2p_1p_2p_3p_4 - 1 = p \leq x$ where the $p_i s$ are primes greater than $x^{1/4-\delta}$.

To count the latter set we use Proposition 4.10. We take $a = 2p_1p_2p_3$, $b = -1$ and $Y = \frac{x+1}{2p_1p_2p_3}$ (since $2p_1p_2p_3p_4 - 1 \leq x \Leftrightarrow p_4 \leq \frac{x+1}{2p_1p_2p_3}$).

By the Proposition 4.10,

$$\begin{aligned} S_{p_4} &= \#\{p_4 \leq Y : ap_4 + b = \text{ prime}\} \\ &= \#\{p_4 \leq \frac{x+1}{2p_1p_2p_3} : 2p_1p_2p_3p_4 - 1 = \text{ prime}\} \\ &\ll \frac{x+1}{2p_1p_2p_3 \log^2 \frac{x+1}{2p_1p_2p_3}} \prod_{\substack{p|2p_1p_2p_3 \\ p\neq 2}} \frac{p-1}{p-2} \end{aligned}$$

Since the p_i's are big primes, the term $\prod_{\substack{p|2p_1p_2p_3 \\ p\neq 2}} \frac{p-1}{p-2}$ is approximately one. Then

$$S_{p_4} \ll \frac{x+1}{2p_1p_2p_3 \log^2 \frac{x+1}{2p_1p_2p_3}}$$

From the fact that for all $i = 1, 2, 3,\ p_i < x^{1/4+3\delta}$ we have for a sufficiently small δ

$$S_{p_4} \ll \frac{1}{p_1p_2p_3 \log^2 \frac{x}{(x^{1/4+3\delta})^3}}$$
$$\ll \frac{1}{p_1p_2p_3} \cdot \frac{x}{\log^2 x^{1/4-9\delta}} \ll (\frac{1}{1/4-9\delta})^2 \frac{1}{p_1p_2p_3} \cdot \frac{x}{\log^2 x}$$

Now we shall sum-up the last term over all possibilities for p_1, p_2, p_3. This number is bounded by

$$S^*_{p_4} = 4\frac{x}{\log^2 x} \sum_{p_1} \frac{1}{p_1} \sum_{p_2} \frac{1}{p_2} \sum_{p_3} \frac{1}{p_3}$$

where the sum is over $x^{1/4-\delta} < p_i < x^{1/4+3\delta}$, $i = 1, 2, 3$.

Observation 4.12. *We have* $\sum\limits_{x^\beta < p < x^\alpha} \frac{1}{p} = \log \frac{\alpha}{\beta}$ *+o(1).*

By observation 4.12,

$$S^*_{p_4} \ll \log^3 \frac{1/4+3\delta}{1/4-\delta} \frac{x}{\log^2 x} \ll \log^3 (1 + \frac{16\delta}{1-4\delta}) \frac{x}{\log^2 x}$$

Since $\log(1+s) = O(s)$ for $0 < s < 1$ and for, $0 < \delta < 1/4, 1-4\delta$ is bounded, we have

$$S^*_{p_4} \ll \delta^3 \frac{x}{\log^2 x}$$

where $\ll$ does not depend on δ. Hence, $S^*_{p_4}$ is a small number in comparison to $S(\mathcal{A}, X^{\frac{1}{4}-\delta}, v) \gg \delta \frac{x}{\log^2 x}$. □

4.2.3. *Second use of Selberg's upper bound sieve.* Up till now we know that for any sufficiently small number $\delta > 0$, there are $c_2(\delta)\frac{x}{\log^2 x}$ primes $p \le x$ such that $\frac{p+1}{2}$ has at most three prime divisors all of which are greater than $x^{1/4-\delta}$. In this section we want to prove the existence of $c_3(\delta)\frac{x}{\log^2 x}$ primes $p \le x$, such that $\frac{p+1}{2} = P_3$ and if $\frac{p+1}{2}$ is a product of exactly three primes $q_3 \ge q_2 \ge q_1$ then $q_1 > x^{1/4-\delta}$, $q_2 > x^{1/4+2\delta}$, $q_3 > x^{1/3+\delta^2}$. First we prove the claim about q_2 (by the previous subsections it is clear that $q_1 > x^{1/4-\delta}$).

Assume that q_1 and q_2 take values between $x^{\frac{1}{4}-\delta}$ and $x^{\frac{1}{4}+2\delta}$. Instead of counting the number of primes $p \le x$ such that $\frac{p+1}{2} = q_1q_2q_3$ where q_1 and q_2 are between $x^{\frac{1}{4}-\delta}$ and $x^{\frac{1}{4}+2\delta}$, we shall count the products

$q_1q_2q_3$ such that $2q_1q_2q_3 - 1 = p \leq x$ where q_1 and q_2 are between $x^{\frac{1}{4}-\delta}$ and $x^{\frac{1}{4}+2\delta}$.

To count this set we use Proposition 4.10. Define $a = 2q_1q_2,\ b = -1$ and $Y = \frac{x+1}{2q_1q_2}$ (since $2q_1q_2q_3 - 1 \leq x \Leftrightarrow q_3 \leq \frac{x+1}{2q_1q_2}$). By Proposition 4.10

$$\begin{aligned} S_{q_3} &= \#\{q_3 \leq Y : aq_3 + b = \text{ prime}\} \\ &= \#\{q_3 \leq \frac{x+1}{2q_1q_2} : 2q_1q_2q_3 - 1 = \text{ prime}\} \\ &\ll \frac{x+1}{2q_1q_2 \log^2 \frac{x+1}{2q_1q_2}} \prod_{\substack{p|2q_1q_2 \\ p\neq 2}} \frac{p-1}{p-2} \end{aligned}$$

As in the previous subsection, since the $q_i's$ are big primes the term $\prod\limits_{\substack{p|2q_1q_2 \\ p\neq 2}} \frac{p-1}{p-2}$ is approximately one, so

$$S_{q_3} \ll \frac{x+1}{2q_1q_2 \log^2 \frac{x+1}{2q_1q_2}} \ .$$

Now we sum-up the last term over all possibilities for q_1, q_2. This number is bounded by, (see the previous subsection)

$$S^*_{q_3} = \frac{x}{\log^2 x} \sum_{x^{\frac{1}{4}-\delta} \leq q_1 \leq x^{\frac{1}{4}+2\delta}} \frac{1}{q_1} \sum_{x^{\frac{1}{4}-\delta} \leq q_2 \leq x^{\frac{1}{4}+2\delta}} \frac{1}{q_2} \ll \frac{x}{\log^2 x} \log^2 \frac{1+8\delta}{1-4\delta}.$$

Since $\log^2 \frac{1+8\delta}{1-4\delta} = O(\delta^2)$, $S^*_{q_3} = O(\delta^2 \frac{x}{\log^2 x})$. Hence for any δ sufficiently small we get a small number of primes $p \leq x$ such that $\frac{p+1}{2} = q_1q_2q_3$ where q_1 and q_2 are between $x^{\frac{1}{4}-\delta}$ and $x^{\frac{1}{4}+2\delta}$. Thus for most such p, we have $q_2 > x^{1/4+2\delta}$.

Finally we prove the claim about q_3. Assume that $\frac{p+1}{2} = q_1q_2q_3,\ q_3 \geq q_2 \geq q_1$ then we have that $q_3 \geq (\frac{p+1}{2})^{\frac{1}{3}}$. The following lemma sharpens this result.

Lemma 4.13. *For any $0 < \delta < 1/4$ there are at most $O(\delta^2 \frac{x}{\log^2 x})$ primes $p \leq x$ for which $(\frac{p+1}{2})^{\frac{1}{3}} \leq q_3 \leq p^{\frac{1}{3}+\delta^2}$ where O does not depend on δ.*

Proof. Note that if $\frac{p+1}{2} \geq \frac{x}{\log^2 x}$ then $q_3 \geq (\frac{p+1}{2})^{\frac{1}{3}} \geq (\frac{x}{\log^2 x})^{\frac{1}{3}} \geq x^{\frac{1}{3}-\delta^2}$ for $x \geq x(\delta)$ (the number of primes p for which $\frac{p+1}{2} \leq \frac{x}{\log^2 x}$, is $o(\frac{x}{\log^2 x})$ by the prime number theorem and so may be ignored).

Assume now that $\frac{p+1}{2} = q_1q_2q_3$ with $x^{1/3-\delta^2} \le q_3 \le x^{1/3+\delta^2}$ and $x^{1/4+2\delta} \le q_2 \le x^{5/12+\delta+\delta^2}$ (this is the maximum range which q_2 can be in). Using Proposition 4.10, we take $a = 2q_2q_3,\ b = -1,\ Y = \frac{x+1}{2q_2q_3}$, and so

$$\begin{aligned} S_{q_1} &= \#\{q_1 \le Y : aq_1 + b = \text{ prime}\} \\ &= \#\{q_1 \le \frac{x+1}{2q_2q_3} : 2q_2q_3 - 1 = \text{ prime}\} \\ &\ll \frac{x+1}{2q_2q_3 \log^2 \frac{x+1}{2q_2q_3}} \prod_{\substack{p|2q_2q_3 \\ p\neq 2}} \frac{p-1}{p-2}. \end{aligned}$$

Since $2x^{3/4+\delta+2\delta^2}$ is the maximum of $2q_2q_3$ ($q_1 > x^{1/4-\delta}$) we obtain

$$S_{q_1} \ll \frac{x}{2q_2q_3 \log^2 \frac{x}{x^{3/4+\delta}}} \ll \frac{x}{q_2q_3 \log^2 x}$$

Now we sum-up the last term over all possibilities for $q_2,\ q_3$. this number is bounded by, (see the proof of Lemma 4.11)

$$\begin{aligned} S^*_{q_1} &= \frac{x}{\log^2 x} \sum_{x^{\frac{1}{4}+2\delta} \le q_2 \le x^{\frac{5}{12}+\delta+\delta^2}} \frac{1}{q_2} \sum_{x^{\frac{1}{3}-\delta^2} \le q_3 \le x^{\frac{1}{3}+\delta^2}} \frac{1}{q_3} \\ &\ll \frac{x}{\log^2 x} \log \frac{5/12+\delta+\delta^2}{1/4+2\delta} \log \frac{1/3+\delta^2}{1/3-\delta^2} \\ &\ll \frac{x}{\log^2 x} \log(1 + \frac{6\delta^2}{1-3\delta^2}) = O(\delta^2 \frac{x}{\log^2 x}) \end{aligned}$$

and for a sufficiently small δ we can ignore this number. □

By the same method (see Lemma 3 in [13]) there are only $O(\delta^2 \frac{x}{\log^2 x})$ primes $p \le x$ such that $\frac{p+1}{2} = r_1 r_2$ where $r_i's$ are primes, $i = 1, 2,\ \ r_2 \ge r_1,\ \ p^{1/2-\delta^2} \le r_1 \le (\frac{p+1}{2})^{1/2}$.

If we summarize this section we conclude that for any sufficiently small $0 < \delta < 1/4$ there are at least $c_3(\delta)\frac{x}{\log^2 x},\ \ c_3(\delta) > 0$, primes $p \le x,\ \ p \equiv u\ (mod\ v)$ such that we can factor $\frac{p+1}{2}$ in at least one of the following ways:

(1) $\frac{p+1}{2}$ is a prime number.
(2) $\frac{p+1}{2} = r_1(p)r_2(p)$ where $r_1(p), r_2(p)$ are some prime numbers, $p^{1/4-\delta} < r_1(p) < p^{1/2-\delta^2},\ p^{1/2+\delta^2} < r_2(p) < p^{3/4+\delta}$.

(3) $\frac{p+1}{2} = q_1(p)q_2(p)q_3(p)$ where $q_1(p) \leq q_2(p) \leq q_3(p)$ are some prime numbers, $q_1(p) > p^{1/4-\delta}$, $q_2(p) > p^{1/4+2\delta}$, $q_3(p) > p^{1/3+\delta^2}$.

4.3. **Proof of Theorem 4.2- The algebraic part.**

4.3.1. *Construction of the arithmetic sequence.* In this section we want to construct integers u and v, $(u,v) = 1$ such that for all primes p such that $p \equiv u \ (mod\ v)$, the discriminants $\Delta_1, ..., \Delta_7$, $\Delta_i \neq 3$ of $\mathbb{Q}(\sqrt{\Delta_1}), ..., \mathbb{Q}(\sqrt{\Delta_7})$, respectively, satisfy

$$(\frac{\Delta_1}{p}) = (\frac{\Delta_2}{p}) = ... = (\frac{\Delta_7}{p}) = -1\ .$$

This means that p is inert simultaneously in all of the fields.

In addition we want to insure that $\frac{p+1}{2}$ will be an odd integer and so we take $u \equiv 1 \ (mod\ 4)$ where $8|v$. Finally, to get $(\frac{p+1}{2}, v) = 1$ we shall construct u and v so that $(\frac{u+1}{2}, v) = 1$ (since after sieving the small factors of $\frac{p+1}{2}$ we may be left with small factors which divide v, see previous section).

In order to fulfill these demands, we will first show that there exist infinitely many primes p with the following simultaneous conditions

$$(4.6) \qquad (\tfrac{-1}{p}) = (\tfrac{3}{p}) = 1 \ \ and \ \ (\tfrac{\Delta_1}{p}) = (\tfrac{\Delta_2}{p}) = ... = (\tfrac{\Delta_7}{p}) = -1$$

This condition is equivalent to the condition:

$$B(p) = (1 + (\frac{-1}{p}))(1 + (\frac{3}{p}))(1 - (\frac{\Delta_1}{p})) \cdots (1 - (\frac{\Delta_7}{p})) \neq 0.$$

Since the Legendre symbol is a multiplicative function, we obtain,

$$B(p) = (1 + (\frac{-1}{p}))(1 + (\frac{3}{p}))(1 - \Sigma(\frac{\Delta_i}{p}) + \Sigma(\frac{\Delta_i\Delta_j}{p}) - ... - (\frac{\Delta_1 \cdots \Delta_7}{p}))$$

Let S be the set of all integers of the form $n = (-1)^{a_1}3^{a_2}\prod_{i=1}^{7}\Delta_i^{b_i}$, $a_i, b_i \in \{0,1\}$. Then

$$(4.7) \qquad \sum_{p \leq Z} B(p) = \sum_{n \in S} (-1)^{b_1 + ... + b_7} \sum_{p \leq Z} (\tfrac{n}{p}), \quad b_i \in \{0,1\}$$

By the assumption in the theorem (see the introduction) each $n \in S$ is not a square when $\sum_{i=1}^{7} b_i$ is odd.

This assumption, together with the fact that for n not a perfect square (by reciprocity law for Legendre symbol),

$$\sum_{p\leq Z}(\tfrac{n}{p}) = o(\pi(Z)) \ \ as\ Z \to \infty$$

implies that $\sum\limits_{p\leq Z} B(p)$ is asymptotic to at least $\pi(Z)$ (since all the negative summands contribute $o(\pi(Z))$ and at least the natural number 1 contributes $\pi(Z)$). This shows that the simultaneous conditions have infinitely many solutions p.

We fix some particular p_0 satisfying the condition. We define $u_2 = p_0$ and for each odd prime l, such that $l|\Delta_1 \cdots \Delta_7$ we define $u_l = p_0$ if $l \nmid p_0 + 1$ and $u_l = 4p_0$ otherwise.

Claim 4.14. *$l \nmid u_l + 1$*

Proof. If $u_l = p_0$ then by the assumption $l \nmid p_0+1$, $l \nmid u_l+1$. If $u_l = 4p_0$, assume, by reductio ad absurdum, that $l|u_l + 1$. Hence $l \mid 4p_0 + 1$. Because $u_l = 4p_0$ and $l \mid p_0 + 1$, we obtain that $l \mid 3p_0$. On the other hand, by our condition, $(\frac{3}{p_0}) = 1$ so $(\frac{p_0}{3}) = 1$ $\ (p_0 \equiv 1\ (mod\ 4))$. Hence $p_0 \equiv 1\ (mod\ 3)$. Since $l \mid p_0 + 1$ and $p_0 \equiv 1\ (mod\ 3)$ we conclude that $l \nmid 3$. Using the assumption that $l \mid p_0 + 1$ we deduce that $l \neq p_0$ (if $l = p_0$ then $l \nmid p_0 + 1$). Hence $l \nmid 3p_0$, a contradiction. □

Let $v = 8\Delta_1 \cdots \Delta_7$ and u be the common solution of $u \equiv u_2\ (mod\ 8)$ and all the congruences $u \equiv u_l\ (mod\ l)$. Such a solution exists, by the Chinese Remainder Theorem.

Since $l \nmid u+1$ for every odd prime $l|v$ and the fact that $u \equiv 1\ (mod\ 4)$ (by the construction $u \equiv u_2\ (mod\ 8)$ where $u_2 = p_0 \equiv 1\ (mod\ 4)$) we conclude that $(\frac{u+1}{2}, v) = 1$. Finally, if $p \equiv u\ (mod\ v)$ then $p \equiv p_0\ (mod\ 8)$ and $p \equiv p_0$ or $4p_0\ (mod\ l)$ for all odd primes $l|v$. So, $(\frac{\Delta_1}{p}) = (\frac{\Delta_1}{p_0}) = -1$, and similarly for all Δ_i's. This completes the construction of u and v.

Note that by the construction of the integers u and v we have that $(u, v) = 1$. (Take l an odd prime number, $l \mid v = 8\Delta_1 \cdots \Delta_7$ and assume that $l \mid u$. Since $u \equiv u_l\ (mod\ l)$, $l \mid u_l$, hence $l \mid p_0$ or $4p_0$; in other words $l = p_0$. But $p_0 \nmid \Delta_1 \cdots \Delta_7$ (p_0 fulfills the simultaneous condition (5.6)) and $l \mid \Delta_1 \cdots \Delta_7$).

4.3.2. *The last step of the proof.* For the last step of the proof we need to use Lemma 4 from Narkiewicz [18], which generalized Lemma 2 in [9];

Lemma 4.15. *If $a_1, \dots a_k$ are multiplicatively independent integers of an algebraic number-field K, G the subgroup of $K^\star$ generated by $a_1, \dots a_k$, and for any prime ideal $\mathbf{P}$ not dividing $a_1, \cdots a_k$ we denote by $G_\mathbf{P}$ the reduction of G $(mod\ \mathbf{P})$, then for all positive y one can have $\#G_\mathbf{P} < y$ for at most $O(y^{1+\frac{1}{k}})$ prime ideals $\mathbf{P}$, with the implied constant being dependent on the a_i's and K.*

Now, as we saw at the end of section 3, for any sufficiently small $0 < \delta < 1/4$ there is some constant $c_3(\delta) > 0$ such that for $c_3(\delta)\frac{x}{\log^2 x}$ primes $p \leq x$, $p \equiv u\ (mod\ v)$ at least one of the following occur:

(1) $\frac{p+1}{2}$ is a prime number.
(2) $\frac{p+1}{2} = r_1(p)r_2(p)$ where $r_1(p), r_2(p)$ are primes so that, $p^{1/4-\delta} < r_1(p) < p^{1/2-\delta^2}$, $\quad p^{1/2+\delta^2} < r_2(p) < p^{3/4+\delta}$.
(3) $\frac{p+1}{2} = q_1(p)q_2(p)q_3(p)$ where $q_1(p) \leq q_2(p) \leq q_3(p)$ are some prime numbers, $q_1(p) > p^{1/4-\delta}$, $q_2(p) > p^{1/4+2\delta}$, $q_3(p) > p^{1/3+\delta^2}$

It is clear by the construction of u and v that $p \equiv 1\ (mod\ 4)$. Because $\#C_\epsilon(p) = p+1$ when p is inert in $\mathbb{Q}(\sqrt{\Delta})$ the unit -1 is a non-square in the group $C_\epsilon(p)$. Hence for any unit ϵ , we can choose constant $c = \pm 1$ such that $c\epsilon$ is a non-square in $C_\epsilon(p)$. Similarly, since $c\epsilon$ is a non-square and the index of the group of squares is 2, the order of $c\epsilon$ is even.

Now we look at our cases:

(1) In this case, by the above note, $c\epsilon$, if not primitive, has order 2 But the number of p's with this property is O(1) (by Lemma 5.7).

(2) Let $c_1\epsilon_1, \dots, c_4\epsilon_4$, be units in the orders $\mathcal{O}_{\Delta_1}, \dots, \mathcal{O}_{\Delta_4}$ of $\mathbb{Q}(\sqrt{\Delta_1})$, $\dots, \mathbb{Q}(\sqrt{\Delta_4})$, $\Delta_i \neq 3$, $i = 1, 2, 3, 4$, respectively. We will show that one of them is primitive for infinitely many primes.

If $\text{ord}(c_i\epsilon_i)\ mod(p) = 2r_1(p) < 2x^{1/2-\delta^2}$ for some $i = 1, 2, 3, 4$ by Lemma 5.7 this occurs for at most $O(x^{1/2-\delta^2})^2 = x^{1-2\delta^2}$

primes $p \leq x$ and this is a negligible number compared to $c_3(\delta)\frac{x}{\log^2 x}$.

Assume $\operatorname{ord}(c_i\epsilon_i)$ $mod(p) = 2r_2(p)$, $i = 1, 2, 3, 4$. Consider the ring of integers $\mathcal{O}_M$ of the compositum field M of $\mathbb{Q}(\sqrt{\Delta_i})$ $i = 1, ..., 4$.

Proposition 4.16. *For any prime ideal $P \mid (p) = p\mathcal{O}_M$:*

$$(\mathcal{O}_M/\mathbf{P})^\star \simeq (\mathcal{O}_{\Delta_1}/p\mathcal{O}_{\Delta_1})^\star \simeq ... \simeq (\mathcal{O}_{\Delta_4}/p\mathcal{O}_{\Delta_4})^\star \ .$$

Proof. Since p is inert in each $\mathbb{Q}(\sqrt{\Delta_i})$, the order of $\mathcal{O}_{\Delta_i}/p\mathcal{O}_{\Delta_i}$ is p^2, i.e., $[\mathcal{O}_{\Delta_i}/p\mathcal{O}_{\Delta_i} : \mathbb{Z}/p\mathbb{Z}] = 2$. Since all these residue fields are finite fields and two finite fields with the same number of elements are isomorphic, it is enough to show that,

$$f = [\mathcal{O}_M/P : \mathbb{Z}/p\mathbb{Z}] = 2.$$

Consider the Galois group $G = Gal[M/\mathbb{Q}]$ and define two subgroups of G, the decomposition group D and the inertia group E:

$$D = D(P|(p)) = \{\sigma \in G | \ \sigma(P) = P\}$$

and

$$E = E(P|(p)) = \{\sigma \in G | \ \sigma(\alpha) \equiv \alpha \ (mod \ P), \ \forall \alpha \in \mathbb{Z}\} \ .$$

Now, consider the Galois group $\bar{G}$,

$$\bar{G} = Gal[\mathcal{O}_M/P \ / \ \mathbb{Z}/p\mathbb{Z}]$$

By [17, beginning of Chapter 4],

$$D/E \simeq \bar{G}$$

By theorem 28 in in [17] (since (p) is inert in all the fields $\mathbb{Q}(\sqrt{\Delta_i})$, (p) is unramified in all the fields $\mathbb{Q}(\sqrt{\Delta_i})$. Hence (p) is also unramified in $\mathcal{O}_M$, i.e., $e =$ the exponent of P in the decomposition of (p), is equal to 1)

$$|E| = e = 1$$

$$|D| = f$$

Immediately we conclude that,

$$D \simeq \bar{G}$$

Since $\bar{G}$ is a cyclic group, we get that D is a cyclic group of order f. But D is a subgroup of G and $G = C_2 \times ... \times C_2$ where C_2 is a group of order 2. So, $f \leq 2$. Since

$$[\mathcal{O}_{\Delta_i}/p\mathcal{O}_{\Delta_i} : \mathbb{Z}/p\mathbb{Z}] = 2$$

we also see that $f \geq 2$. Hence $f = 2$.

Because the compositum of normal extensions is normal, this claim is true for all the prime ideals P in the decomposition of (p) (they have the same e and the same f) □

By Proposition 4.16 $| < c_1\epsilon_1, c_2\epsilon_2, c_3\epsilon_3, c_4\epsilon_4 > | = 2r_2(p) \ll p^{3/4+\delta}$ in $(\mathcal{O}_M/\mathbf{P})^\star$ for $(p)|P$ (this is a cyclic group). By Lemma 5.7 the number of $p \leq x$ that have this order is at most $O(x^{3/4+\delta})^{\frac{5}{4}} = O(x^{15/16+5\delta/4})$ but we can choose δ to be as small as needed. Hence the number of primes p, $p \leq x$ such that $c_i\epsilon_i$ $i = 1, ..., 4$ have order $2r_2(p)$ is a small in comparison with $c_3(\delta)\frac{x}{\log^2 x}$.

(3) Denote by $S_{(1,n)}$ the set $\{c_1\epsilon_1, ..., c_n\epsilon_n\}$ where $c_1\epsilon_1, ..., c_n\epsilon_n$ are multiplicatively independent units and take four units $c_{i_1}\epsilon_{i_1}, ..., c_{i_4}\epsilon_{i_4}$ from $S_{(1,n)}$ and assume that $q_1(p)$, which is greater than $x^{1/4-\delta}$, divides $[C_\epsilon(p) : \langle c_{i_k}\bar{\epsilon}_{i_k}\rangle]$ for $k = 1, ..., 4$.

For any unit ϵ let be $\bar{\epsilon}$ its image in $C_\epsilon(p)$. Then $|\langle c_{i_k}\bar{\epsilon}_{i_k}\rangle| = \frac{p+1}{[C_\epsilon(p):\langle c_{i_k}\bar{\epsilon}_{i_k}\rangle]} \ll p^{3/4+\delta} \ll x^{3/4+\delta}$ for $k = 1, ..., 7$. Since $q_1(p)$ divides $[C_\epsilon(p) : \langle c_{i_k}\bar{\epsilon}_{i_k}\rangle]$ for $k = 1, ..., 4$ and $C_\epsilon(p)$ is a cyclic group, $|\langle c_{i_1}\epsilon_{i_1}, ..., c_{i_4}\epsilon_{i_4}\rangle|$ *mod* $p \ll x^{3/4+\delta}$. By Lemma 5.7 it occurs in at most $O((x^{3/4+\delta})^{5/4}) = O(x^{15/16+5\delta/4})$ primes $p \leq x$ which is a negligible number relatively to $c_3(\delta)\frac{x}{\log^2 x}$ for sufficiently small δ.

So, for at most three units from $c_{i_1}\epsilon_{i_1}, ..., c_{i_4}\epsilon_{i_4}$, $q_1(p)$ divides $[C_\epsilon(p) : \langle c_{i_k}\bar{\epsilon}_{i_k}\rangle]$ for $k = 1, ..., 4$. In other words for at most three from $c_{i_1}\epsilon_{i_1}, ..., c_{i_4}\epsilon_{i_4}$ $q_1(p)$ does not divide $|\langle c_{i_k}\bar{\epsilon}_{i_k}\rangle|$. Hence for at least one unit, say $c_n\epsilon_n$, $q_1(p)$ divide $|\langle c_n\bar{\epsilon}_n\rangle|$.

Denote by $S_{(1,n-1)}$ the set $\{c_1\epsilon_1, ..., c_{n-1}\epsilon_{n-1}\}$. By repeating the former process for $S_{(1,n-1)}$ we obtain that for at least one integer, say $c_{n-1}\epsilon_{n-1}$, $q_1(p)$ divide $|\langle c_{n-1}\bar{\epsilon}_{n-1}\rangle|$.

We continue this process till we obtain the set $S_{(4,n)} = \{c_4\epsilon_4, ..., c_n\epsilon_n\}$ where $c_4\epsilon_4, ..., c_n\epsilon_n$ are multiplicatively independent units such that $q_1(p)$ divides $|\langle c_t\bar{\epsilon}_t\rangle|$ for $t = 4, ..., n$.

Now, we are repeating the process which we use to $q_1(p)$ and $S_{(1,n)}$ for $q_2(p) > p^{1/4+2\delta}$ and the set $S_{(4,n)} = \{c_4\epsilon_4, ..., c_n\epsilon_n\}$. Take three units $c_{i_1}\epsilon_{i_1}, ..., c_{i_3}\epsilon_{i_3}$ from $S_{(4,n)}$ and assume that $q_2(p)$, which is greater than $x^{1/4+2\delta}$, divides $[C_\epsilon(p) : \langle c_{i_k}\bar{\epsilon}_{i_k}\rangle]$ for $k = 1, 2, 3$.

Then $|\langle c_{i_k}\bar{\epsilon}_{i_k}\rangle| = \frac{p+1}{[C_\epsilon(p):\langle c_{i_k}\bar{\epsilon}_{i_k}\rangle]} \ll p^{3/4-2\delta} \ll x^{3/4-2\delta}$ for $k = 1, 2, 3$. Since $q_2(p)$ divides $[C_\epsilon(p) : \langle c_{i_k}\bar{\epsilon}_{i_k}\rangle]$ for $k = 1, 2, 3$ and $C_\epsilon(p)$ is a cyclic group, $|\langle c_{i_1}\epsilon_{i_1}, ..., c_{i_3}\epsilon_{i_3}\rangle|$ *mod p* $\ll x^{3/4+\delta}$. By Lemma 5.7 it occurs in at most $O((x^{3/4-2\delta})^{4/3}) = O(x^{1-8\delta/3})$ primes $p \leq x$ which is a negligible number relatively to $c_3(\delta)\frac{x}{\log^2 x}$ for sufficiently small δ.

So, for at most two units from $c_{i_1}\epsilon_{i_1}, ..., c_{i_3}\epsilon_{i_3}$, $q_2(p)$ divides $[C_\epsilon(p) : \langle c_{i_k}\bar{\epsilon}_{i_k}\rangle]$ for $k = 1, 2, 3$. In other words for at most two from $c_{i_1}\epsilon_{i_1}, ..., c_{i_3}\epsilon_{i_3}$, $q_2(p)$ does not divide $|\langle c_{i_k}\bar{\epsilon}_{i_k}\rangle|$. Hence for at least one integer, say $c_n\epsilon_n$, $q_2(p)$ divide $|\langle c_n\bar{\epsilon}_n\rangle|$.

Denote by $S_{(4,n-1)}$ the set $c_4\epsilon_4, ..., c_{n-1}\epsilon_{n-1}$. By repeating the former process for S_{n-1} we obtain that for at least one unit, say ϵ_{n-1}, $q_2(p)$ divide $|\langle\bar{\epsilon}_{n-1}\rangle|$.

We continue this process till we obtain the set $S_{(6,n)} = \{c_6\epsilon_6, ..., c_n\epsilon_n\}$ where $c_6\epsilon_6, ..., c_n\epsilon_n$ are multiplicatively independent units such that $q_2(p)$ divides $|\langle c_t\bar{\epsilon}_t\rangle|$, $t=6,...,n$ and in fact $q_1(p)q_2(p)$ divides $|\langle c_t\bar{\epsilon}_t\rangle|$ for $t=6,...,n$.

Finally, We repeating this process for $q_3(p) > p^{1/3+\delta^2}$ and the set $S_{(6,n)}=\{c_6\epsilon_6,...,c_n\epsilon_n\}$. Take two units $c_{i_1}\epsilon_{i_1}, c_{i_2}\epsilon_{i_2}$ from $S_{(6,n)}$ and assume that $q_3(p)$, which is greater than $x^{1/3+\delta^2}$, divides $[C_\epsilon(p):\langle c_{i_k}\bar{\epsilon}_{i_k}\rangle]$ for $k=1,2$.

Then $|\langle c_{i_k}\bar{\epsilon}_{i_k}\rangle| = \frac{p+1}{[C_\epsilon(p):\langle c_{i_k}\bar{\epsilon}_{i_k}\rangle]} \ll p^{2/3-\delta^2} \ll x^{2/3-\delta^2}$, $k=1,2$. Since $q_3(p)$ divides $[C_\epsilon(p):\langle c_{i_k}\bar{\epsilon}_{i_k}\rangle]$ for $k=1,2$ and $C_\epsilon(p)$ is a cyclic group, $|\langle c_{i_1}\epsilon_{i_1}, c_{i_2}\epsilon_{i_2}\rangle|\ mod\ p \ll x^{2/3-\delta^2}$. By Lemma 5.7 it occurs in at most $O((x^{2/3-\delta^2})^{3/2}) = O(x^{1-3\delta^2/2})$ primes $p\le x$ which is a negligible number relatively to $c_3(\delta)\frac{x}{\log^2 x}$ for sufficiently small δ.

So, for at most one unit from $c_{i_1}\epsilon_{i_1}, c_{i_2}\epsilon_{i_2}$, $q_3(p)$ divides $[C_\epsilon(p):\langle c_{i_k}\bar{\epsilon}_{i_k}\rangle]$ for $k=1,2$. In other words for at most one from $c_{i_1}\epsilon_{i_1}, c_{i_2}\epsilon_{i_2}$ $q_3(p)$ does not divide $|\langle c_{i_k}\bar{\epsilon}_{i_k}\rangle|$. Hence for at least one integer, say $c_n\epsilon_n$, $q_3(p)$ divide $|\langle c_n\bar{\epsilon}_n\rangle|$.

Denote by $S_{(6,n-1)}$ the set $\{c_6\epsilon_6,...,c_{n-1}\epsilon_{n-1}\}$. By repeating the former process for S_{n-1} we obtain that for at least one unit, say ϵ_{n-1}, $q_3(p)$ divide $|\langle\bar{\epsilon}_{n-1}\rangle|$.

We continue this process till we obtain the set $S_{(7,n)}=\{c_7\epsilon_7,...,c_n\epsilon_n\}$ where $c_7\epsilon_7,...,c_n\epsilon_n$ are multiplicatively independent units such that $q_3(p)$ divides $|\langle c_t\bar{\epsilon}_t\rangle|$ for $t=7,...,n$ and in fact $q_1(p)q_2(p)q_3(p)$ divides $|\langle c_t\bar{\epsilon}_t\rangle|$ for $t=7,...,n$.

Hence if we take $n=7$ multiplicatively independent integers we obtain that one of them have at least the order $\frac{p+1}{2}$. Since we choose the $c_j's$ such that the $c_j\epsilon_j's$ are quadratics non-residue we obtain that one of them have at least the order $p+1$ which completes the proof of the Theorem 4.2

Note that Theorem 4.2 implies Corollary 4.3.

5. Artin's conjecture for nonunits

In this chapter we want to extend the result of the previous chapter for any algebraic integer modulo inert primes p. We will prove

Theorem 5.1. *Let $K = \mathbb{Q}(\sqrt{\Delta})$ be a quadratic field and $\{\alpha_i\}_{i=1}^{85}$ be a set of 85 integers of K such that*

1. *$N(\alpha_i) = \alpha_i \sigma(\alpha_i)$, the norms of the $\alpha_i's$, are multiplicatively independent.*

2. *$5N(\alpha_i)\Delta$, $N(\alpha_i)$ are not perfect squares.*

3. *$M(\alpha_i) = \sigma(\alpha_i)/\alpha_i$ are multiplicatively independent.*

Then at least one of the 85 integers has at least order $\frac{p^2-1}{24}$ mod p for infinitely many inert primes p in K.

Note that in the case of split primes, Narkiewicz ([18]) proved a much stronger result.

Since in our case the order is $p^2 - 1$, which is not "linear", their divisors are too big and we can not use the method of [12]. But since $p^2 - 1 = (p-1)(p+1)$ can be factored into two linear factors, with the following remark we can still use the method of [12]

Remark 5.2. *Consider an algebraic number α in $K = \mathbb{Q}(\sqrt{\Delta})$. Let $p \nmid \alpha$ be an inert prime in K. Since:*

(1) $M(\alpha) \equiv \alpha^{p-1}$ (mod (p))

(2) $N(\alpha) \equiv \alpha^{p+1}$ (mod (p))

We have:

$ord(M(\alpha)) \mid ord(\alpha)\ (mod\ (p))$ *and* $ord(N(\alpha)) \mid ord(\alpha)\ (mod\ (p))$

In addition:

$ord(M(\alpha)) \mid p+1$ *and* $ord(N(\alpha)) \mid p-1$
But,

$(\frac{p-1}{2}, p+1) = 1$ *or* $(p-1, \frac{p+1}{2}) = 1$

So,

$ord(M(\alpha))ord(N(\alpha)) \mid 2ord(\alpha)\ \ (mod\ (p))$

Let e_1 and e_2 be some integers. If we prove that, $M(\alpha)$ and $N(\alpha)$ have simultaneously at least orders $\frac{p+1}{e_1}$ and $\frac{p-1}{e_2}$, respectively, then we will obtain that α have at least order $\frac{p^2-1}{2e_1e_2}$. With this way we reduce the problem to a "linear" problem.

As in the former chapter we need to decide on some notation for the lemma from sieve methods.

5.1. **Notation and Preliminaries.** Let $\pi(y; m, s)$ denote the number of primes $p \leq y$ such that $p \equiv s\ (mod\ m)$ where m and s are some integers, and

$$E(y; m, s) := \pi(y; m, s) - \frac{Li(y)}{\varphi(m)}$$

where $Li(y) = \int_2^y \frac{dt}{\log t}$. Also set

$$E(x; m) := \max_{1 \leq y \leq x} \max_{(s,m)=1} |E(y; m, s)|\ .$$

Define $\mathcal{A} = \{p^2 - 1 | p \leq x, p \equiv u\ (mod\ v)\}$ where $u,\ v$ are some given integers such that $(u, v) = 1$ and take $X = \frac{Li(x)}{\varphi(v)}$.

For a square-free integer d, $(d,v)=1$, denote

$$\begin{aligned}|\mathcal{A}_d| &:= |\{a\in\mathcal{A} : a\equiv 0 \mod d\}|\\ &= |\{p^2-1 : p\le x,\ p\equiv u \mod v,\ p^2-1\equiv 0 \mod d\}|\\ &= \sum_{\substack{m=1\\ m^2-1\equiv 0 \mod d}}^{d} |\{p|p\le x, p\equiv u \mod v,\ p\equiv m \mod d\}|\\ &= \sum_{\substack{m=1\\ m^2-1\equiv 0 \mod d\\ (m,d)=1}}^{d} |\{p|p\le x, p\equiv u \mod v,\ p\equiv m \mod d\}|\end{aligned}$$

By the Chinese Remainder Theorem, for each m there exists an integer l_m such that

$$|\mathcal{A}_d| = \sum_{\substack{m=1\\ m^2-1\equiv 0 \mod d\\ (m,d)=1}}^{d} |\{p|p\le x,\ p\equiv l_m\ (mod\ dv)\}|;$$

Since $|\{p|p\le x,\ p\equiv l_m\ (mod\ dv)\}|$ is asymptotically independent of m, there exists some integer l such that

$$|\mathcal{A}_d| = \pi(x;dv,l) \sum_{\substack{m=1\\ m^2-1\equiv 0 \mod d\\ (m,d)=1}}^{d} 1 = \pi(x;dv,l)\rho(d)$$

where $\rho(d) = \sum_{\substack{m=1\\ m^2-1\equiv 0 \mod d\\ (m,d)=1}}^{d} 1.$

We note that for any prime q, $\rho(q)=2$ and hence for any square-free d, $\rho(d)=2^{\nu(d)}$ where $\nu(d)$ denotes the number of prime divisors of d.

By the definition of $E(x;dv,l)$,

$$|\mathcal{A}_d| = \frac{\rho(d)}{\varphi(d)}\frac{Lix}{\varphi(v)} + \rho(d)E(x;dv,l)) = \frac{2^{\nu(d)}}{\varphi(d)}X + 2^{\nu(d)}E(x;dv,l)$$

For any prime q define $\omega(q) := \frac{2q}{\varphi(q)}$, $\omega(d) = \prod\limits_{q|d} \omega(q) = \frac{2^{\nu(d)}d}{\varphi(d)}$ and

$$R_d := |\mathcal{A}_d| - \frac{\omega(d)}{d} X = 2^{\nu(d)} E(x; dv, l)$$

Finally, we define the M$\ddot{o}$bius function, $\mu(1) = 1$ and for a square-free $d = p_1 \cdots p_k$, $\mu(d) = (-1)^k$.

Now we want to prove two lemmas.

Lemma 5.3. *For any prime $q > 3$ which is relatively prime to v we have:*

$$0 \leq \frac{2}{q-1} \leq \frac{1}{2}. \tag{5.1}$$

$$\sum_{w \leq q < z} \frac{2}{q-1} \log q - 2 \log \frac{z}{w} = O(1) \quad (2 \leq w \leq z) \tag{5.2}$$

where O does not depend on z or w.

$$\prod_{\substack{2<q<z \\ q \nmid v}} (1 - \frac{2}{q-1}) \gg \frac{1}{\log^2 z}. \tag{5.3}$$

Proof. Since $q > 3$, it is clear that (7.3) holds.

As for the second equation, $\sum\limits_{w \leq q < z} \frac{2}{q-1} \log q = 2 \sum\limits_{w \leq q < z} \frac{\log q}{q} \frac{q}{q-1} = 2 \sum\limits_{w \leq q < z} \frac{\log q}{q}(1 + \frac{1}{q-1}) = 2 \sum\limits_{w \leq q < z} \frac{\log q}{q} + 2 \sum\limits_{w \leq q < z} \frac{\log q}{q(q-1)} = 2 \log \frac{z}{w} + O(1) \qquad (\sum\limits_{p<x} \frac{\log p}{p} = \log x + O(1))$.

Hence we get (7.4). Finally,

$$\prod_{\substack{2<q<z\\ q\nmid v}} (1-\frac{2}{q-1}) \gg \prod_{2<q<z} (1-\frac{2}{q-1})$$

$$\begin{aligned}&= \exp(\log \prod_{2<q<z} (1-\frac{2}{q-1}))\\ &= \exp(\sum_{2<q<z} \log(1-\frac{2}{q-1}))\\ &\gg \exp(\sum_{2<q<z} (-\frac{2}{q-1}-\frac{4}{(q-1)^2}))\end{aligned}$$

Since

$$\frac{2}{q-1} = \frac{2}{q} + \frac{2}{q(q-1)} \leq \frac{2}{q} + \frac{2}{(q-1)^2}$$

and $\sum\limits_{2<q<z} \frac{2}{(q-1)^2}$ converges, we get

$$\prod_{2<q<z} (1-\frac{2}{q-1}) \gg \exp(-\sum_{2<q<z} \frac{2}{q})$$

Since

$$\sum_{2<q<z} \frac{2}{q} \sim 2\log\log z$$

we have

$$\exp(-\sum_{2<q<z} \frac{2}{q}) \gg \exp(-2\log\log z) = \frac{1}{\log^2 z}$$

□

Lemma 5.4. *For any square-free natural number d, $(d, v) = 1$, and a real number $A > 0$, there exist constants $c_2(\geq 1)$ and $c_3(\geq 1)$ such that*

$$\sum_{d<\frac{X^{\frac{1}{2}}}{(\log x)^{c_2}}} \mu^2(d)3^{\nu(d)}|R_d| \leq c_3\frac{X}{\log^A X}, \quad (X \geq 2) \tag{5.4}$$

Proof. (See Lemma 4.5) Denote by S_{R_d} the term which we need to estimate.

$$S_{R_d} = \sum_{d<\frac{X^{\frac{1}{2}}}{(\log x)^{c_2}}} \mu^2(d)3^{\nu(d)}|R_d|$$

By the definitions of R_d and $E(x;dv)$

$$S_{R_d} \leq \sum_{d<\frac{X^{\frac{1}{2}}}{(\log x)^{c_2}}} \mu^2(d)6^{\nu(d)}|E(x;dv)|.$$

Since $E(x;dv) \ll \frac{x}{dv}$ if $d \leq \frac{x}{v}$, we get that

$$S_{R_d} \ll x^{\frac{1}{2}} \sum_{d<\frac{X^{\frac{1}{2}}}{(\log x)^{c_2}}} \frac{\mu^2(d)6^{\nu(d)}}{d^{\frac{1}{2}}}|E(x;dv)|^{\frac{1}{2}}.$$

By Cauchy's Inequality,

$$S_{R_d} \ll x^{\frac{1}{2}}(\sum_{d<X^{\frac{1}{2}}} \frac{\mu^2(d)6^{2\nu(d)}}{d})^{\frac{1}{2}}(\sum_{dv<\frac{vX^{\frac{1}{2}}}{(\log x)^{c_2}}} |E(x;dv)|)^{\frac{1}{2}}.$$

For sufficiently large x we obtain

$$S_{R_d} \ll x^{\frac{1}{2}}(\sum_{d<x^{\frac{1}{2}}} \frac{\mu^2(d)6^{2\nu(d)}}{d})^{\frac{1}{2}}(\sum_{dv<\frac{x^{\frac{1}{2}}}{(\log x)^{c_2}}} |E(x;dv)|)^{\frac{1}{2}}.$$

With Bombieri-Vinogradov Theorem ([5]) (given any positive constant e_1, there exists a positive constant e_2 such that $\sum_{d<\frac{x^{\frac{1}{2}}}{\log^{e_2} x}} E(x;d) = O(\frac{x}{\log^{e_1} x})$) for the last sum and the inequality $\sum_{d<w} \frac{\mu^2(d)36^{\nu(d)}}{d} \leq (\log w + 1)^{36}$ (see [11], p.115, equation (6.7)) we find that for given constant B there exists c_2 such that

$$S_{R_d} \ll \frac{x}{\log^B x}.$$

So, for given A there exists c_2 such that

$$S_{R_d} \ll \frac{X}{\log^A X}$$

where $\ll$ depends on v and c_2. □

5.2. **Proof of Theorem 5.1 - the sieve part.** In this section we use the Selberg lower bound sieve and show that there is some small real number δ_1 and some constant $c(\delta_1) > 0$ (which depends on δ_1) such that for at least $c(\delta_1)\frac{x}{\log^3 x}$ primes $p \leq x,\ p \equiv u\ (mod\ v)$, if $q|p^2-1$ then either $q > x^{1/8+\delta_1}$ or $q|v$.

Now, define $S(\mathcal{A}, z, v) = |\{a|a \in \mathcal{A}, (a, \prod_{\substack{p<z \\ p\nmid v}} p) = 1\}|$ and define a function g by $g(t_0) = 1, t_0 = 4.42$ and $g(t) < 1$ for $t > t_0$. Then (see [11, Theorem 7.4, page 219]):

Lemma 5.5. *We have*

$$(5.5)\ \ S(\mathcal{A}, z, v) \geq X \prod_{\substack{q<z \\ q\nmid v}} (1 - \frac{\omega(q)}{q})\{1 - g(\frac{\log X}{2\log z}) + O(\frac{(loglog3X)^8}{logX})\}$$

where the O-term does not depend on X or on z.

By Lemmas 5.3 and 4.5, (7.3), (7.4) and (5.4) hold. Hence we can use Lemma 5.5 with $z = X^{\frac{1}{8}+\delta_0}$

$$S(\mathcal{A}, X^{\frac{1}{8}+\delta_0}, v) \geq X \prod_{\substack{q<X^{\frac{1}{8}+\delta_0} \\ q\nmid v}} (1 - \frac{2}{q-1})\{1 - g(\frac{1}{2}\frac{\log X}{\log X^{\frac{1}{8}+\delta_0}}) + O(\frac{(loglog3X)^8}{logX})\}.$$

By Lemma 5.3 (5.3) we have for δ_0 sufficiently small

$$S(\mathcal{A}, X^{\frac{1}{8}+\delta_0}, v) \gg \frac{X}{\log^2 X} \gg \frac{x}{\log^3 x}$$

Thus for such δ_0 we obtain that there is a constant $c(\delta_0) > 0$ (which depends on δ_0) such that for at least $c(\delta_0)\frac{x}{\log^3 x}$ primes $p \leq x,\ p \equiv u\ (mod\ v)$ if $q|p^2-1$ then either $q > x^{1/8+\delta_0}$ or $q|v$. Hence we obtain that for all $0 < \delta_1 < \delta_0$ there is a constant $c(\delta_1) > 0$ (which depends on δ_1) such that for at least $c(\delta_1)\frac{x}{\log^3 x}$ primes $p \leq x,\ p \equiv u\ (mod\ v)$, if $q|p^2-1$ then either $q > x^{1/8+\delta_1}$ or $q|v$.

5.3. **Proof of Theorem 5.1 - The algebraic part.**

5.3.1. *Construction of the arithmetic sequence.* Let $K = Q(\sqrt{\Delta})$ be any quadratic field, $\mathcal{O}$ the integers ring of K, $\alpha \in \mathcal{O}$ any algebraic integer and $a = N(\alpha)$. In this section we want to construct integers u

and v, $(u, v) = 1$ such that for all primes p such that $p \equiv u\ (mod\ v)$, the discriminant Δ of $\mathbb{Q}(\sqrt{\Delta})$ and a satisfy

$$(\frac{\Delta}{p}) = (\frac{a}{p}) = -1.$$

This means that p is inert and a is not a quadratic residue $(mod\ p)$. In addition we want to obtain by the construction that $(\frac{p^2-1}{24}, v) = 1$ (since after sieving the small factors of $\frac{p^2-1}{24}$ we may be left with small factors which divide v, see previous section).

In order to fulfill these demands, we will first show that there exist infinitely many primes p satisfying the following simultaneous conditions

$$(\tfrac{-1}{p}) = (\tfrac{5}{p}) = (\tfrac{a}{p}) = (\tfrac{\Delta}{p}) = -1 \tag{5.6}$$

This condition is equivalent to the condition:

$$B(p) = (1 - (\frac{-1}{p}))(1 - (\frac{5}{p}))(1 - (\frac{a}{p}))(1 - (\frac{\Delta}{p})) \neq 0$$

Since the Legendre symbol is a multiplicative function, we obtain,

$$(1 - (\frac{-1}{p}))(1 - (\frac{a}{p}) - (\frac{\Delta}{p}) + (\frac{a\Delta}{p}) - (\frac{5}{p}) + (\frac{5a}{p}) + (\frac{5\Delta}{p}) - (\frac{5a\Delta}{p}))$$

Let S be the set of all integers of the form $n = (-1)^{b_0} 5^{b_1} a^{b_2} \Delta^{b_3}$, $b_i \in \{0, 1\}$. Then

$$\sum_{p \leq Z} B(p) = \sum_{n \in S} (-1)^{b_0 + b_1 + b_2 + b_3} \sum_{p \leq Z} (\tfrac{n}{p}), \quad b_i \in \{0, 1\} \tag{5.7}$$

By the assumption in the theorem each $n \in S$ is not a perfect square when $\sum\limits_{i=0}^{3} b_i$ is odd.

This assumption, together with the fact that for n not a perfect square (by reciprocity law for Legendre symbol)

$$\sum_{p \leq Z} (\tfrac{n}{p}) = o(\pi(Z)) \ \ as\ Z \to \infty$$

implies that $\sum\limits_{p \leq Z} B(p)$ is asymptotic to at least $\pi(Z)$ (since all the negative summands contribute $o(\pi(Z))$ and at least the natural number 1 contributes $\pi(Z)$). This shows that the simultaneous conditions have infinitely many solutions p.

We fix some particular p_0 satisfying the condition (5.6) and for each odd prime $l \neq 3$, such that $l|24a\Delta$ we define $u_l = p_0$ if $l \nmid p_0^2 - 1$, and $u_l = 9p_0$ otherwise.

Claim 5.6. $l \nmid u_l^2 - 1$

Proof. If $u_l = p_0$ then by the assumption $l \nmid p_0^2 - 1$, so $l \nmid u_l^2 - 1$. If $u_l = 9p_0$, assume, by reductio ad absurdum, that $l|u_l^2 - 1$. Hence $l \mid 81p_0^2 - 1$. Since, $l \mid p_0^2 - 1$, we obtain that $l \mid 80p_0^2$. On the other hand, by our condition, $(\frac{5}{p_0}) = -1$ so $(\frac{p_0}{5}) = -1$ $(p_0 \equiv 1\ (mod\ 4))$. Hence $p_0 \equiv 2$ or $3\ (mod\ 5)$. Since $l \mid p_0^2 - 1$ and $p_0 \equiv 2$ or $3\ (mod\ 5)$ we conclude that $l \nmid 5$. Using the assumption that $l \mid p_0^2 - 1$ we deduce that $l \neq p_0$ (if $l = p_0$ then $l \nmid p_0^2 - 1$). Hence $(l \neq 2, 3)$ $l \nmid 80p_0^2$, which is a contradiction. □

In addition let $u_2 = p_0$ if $8 \mid {p_0}^2 - 1$ and $u_2 = p_0 - 8$ if $16 \mid {p_0}^2 - 1$. Likewise we take $u_3 = p_0$ if $3 \mid {p_0}^2 - 1$ and $u_3 = p_0 - 3$ if $9 \mid {p_0}^2 - 1$.

Let $v = 24a\Delta$ and u be the common solution of $u \equiv u_2\ (mod\ 16)$, $u \equiv u_3\ (mod\ 9)$ and all the congruences $u \equiv u_l\ (mod\ l)$. Such a solution exists, by the Chinese Remainder Theorem.

Since $l \nmid u^2 - 1$ for every odd prime $l \neq 2, 3,\ l \mid v$, and by the construction $(\frac{u^2-1}{24}, 6) = 1$ we conclude that $(\frac{u^2-1}{24}, v) = 1$.

Finally, if $p \equiv u\ (mod\ v)$, then $p \equiv p_0\ (mod\ 24)$ and $p \equiv p_0$ or $4p_0\ (mod\ l)$ for all odd primes $l|v$. So, $(\frac{\Delta}{p}) = (\frac{\Delta}{p_0}) = -1$, and similarly for a. This completes the construction of u and v.

Note that by the construction of the integers u and v we have that $(u, v) = 1$. (take l an odd prime number, $l \mid v = 24a\Delta$ and assume that $l \mid u$. Since $u \equiv u_l\ (mod\ l)$, $l \mid u_l$. Hence $l \mid p_0$ or $9p_0$ (in this case $l \neq 2, 3$). In other words $l = p_0$. But $p_0 \nmid 24a\Delta$ (p_0 fulfills the simultaneous condition (5.6)) and $l \mid 24a\Delta$).

5.3.2. *The last step of the proof.* As we saw at the previous subsections, for at least $c(\delta_1)\frac{x}{\log^3 x}$ primes $p \leq x,\ p \equiv u\ (mod\ v)$, if $q|p^2 - 1$

then $q > x^{1/8+\delta_1}$ or $q|v$. Since $(\frac{p^2-1}{24}, v) = 1$, if $q|\frac{p^2-1}{24}$ then $q > x^{1/8+\delta_1}$.

Since by the construction of u and v, $p \equiv 1$ $(mod\ 4)$ and $(\frac{p^2-1}{24}, v) = 1$, we have that $\frac{p-1}{4}$ and $\frac{p+1}{2}$ are odd. In addition if $p \equiv 1$ $(mod\ 3)$ then $(\frac{p-1}{12}, v) = 1$ and if $p \equiv -1$ $(mod\ 3)$ then $(\frac{p+1}{6}, v) = 1$

If we conclude the result about $p - 1$ and $p + 1$ we have for at least $c_1(\delta_1)\frac{x}{\log^3 x}$ primes $p \leq x,\ p \equiv u\ (mod\ v)$, if $q \mid \frac{p-1}{d_-}$ or $q \mid \frac{p+1}{d_+}$ then $q > x^{1/8+\delta_1}$, where $d_- = 4$ or 12 and $d_+ = 6$ or 2, respectively.

For the last step of the proof we need to use a version of Lemma 4 from Narkiewicz [18], which generalized Lemma 2 in [9].

Lemma 5.7. *If $a_1, \ldots a_k$ are multiplicatively independent algebraic numbers of an algebraic number-field K, G the subgroup of $K^\star$ generated by $a_1, \ldots a_k$, and for any prime ideal $\mathbf{P}$ not dividing $a_1, \cdots a_k$ we denote by $G_\mathbf{P}$ the reduction of G $(mod\ \mathbf{P})$, then for all positive y one can have $|G_\mathbf{P}| < y$ for at most $O(y^{1+\frac{1}{k}})$ prime ideals $\mathbf{P}$, with the implied constant being dependent on the a_i's and K.*

Proof. According to [18],

For any real number T denote by $M = M(T)$ the set of all k-element sequences $(r_1, ..., r_k)$ of non-negative integers satisfying

$$|r_1| + |r_2| + ... + |r_k| \leq T$$

It is easy to see that for T tending to infinity $|M(T)| = (c + o(1))T^k$ with suitable positive constant $c = c_k$. If now P is a prime ideal for which $|G_P| < y$, then select T to be the smallest rational integer with $cT^k > 2y$ and let $a_i = \frac{b_i}{c_i}$ for $i = 1, ..., k$. There exist two distinct sequences $Z = (z_i),\ W = (w_i)$ in $M(T)$ for which

$$P|\frac{b_1^{z_1} \cdots b_k^{z_k}}{c_1^{z_1} \cdots c_k^{z_k}} - \frac{b_1^{w_1} \cdots b_k^{w_k}}{b_1^{w_1} \cdots c_k^{w_k}}$$

Hence for sufficient large P (since the $a_i's$ are multiplicatively independent).

$$P|\frac{b_1^{z_1}\cdots b_k^{z_k}-b_1^{w_1}\cdots b_k^{w_k}}{c_1^{[z_1,w_1]}\cdots c_k^{[z_k,w_k]}}=D\neq 0$$

Thus for sufficient large P

$$\nu_P(\Pi a_i^{z_i-w_i}-1)\geq 0$$

where ν_P denotes the P-adic valuation and it follows that for fixed $z_1-w_1,...,z_k-w_k$ we obtain $\ll \log{(max_j|\bar{a_j}|^{2T})}\ll T$ possibilities for P. Finally we obtain

$$|\{P|\ |G_P|<y\}|\ll T^{1+k}\ll y^{1+\frac{1}{k}}$$

□

Look at the $p-1$ case (the case of $p+1$ is similar). We have for at least $c_1(\delta_1)\frac{x}{\log^3 x}$ primes $p\leq x,\ p\equiv u\ (mod\ v)$ such that if $q\mid\frac{p-1}{d_-}$ then $q>x^{1/8+\delta_1}$ where $d_-=4$ or 12. Let $p-1=d_-q_1(p)q_2(p)\cdots q_m(p),\ q_m(p)>q_{m-1}(p)>...>q_1(p),\ m\leq 7$, and let a be some integer where $\bar{a}$ its image in $\mathbb{F}_p^*$.

Denote by S_n the set $S_n=\{a_1,...,a_n\}$ where $a_1,...,a_n$ are multiplicatively independent integers and take seven integers $a_{i_1},...,a_{i_7}$ from S_n and assume that at least one prime, say $q_1(p)$, which is greater than $x^{1/8+\delta_1}$, divides $[\mathbb{F}_p^*:\langle\bar{a}_{i_k}\rangle]$ for $k=1,...,7$.

Then $|\langle\bar{a}_{i_k}\rangle|=\frac{p-1}{[\mathbb{F}_p^*:\langle\bar{a}_{i_k}\rangle]}\ll p^{7/8-\delta_1}\ll x^{7/8-\delta_1},\quad k=1,...,7$. Since $q_1(p)$ divides $|\mathbb{F}_p^*:\langle\bar{a}_{i_k}\rangle|$ for $k=1,...,7$ and $\mathbb{F}_p^*$ is a cyclic group, $|\langle a_{i_1},...,a_{i_7}\rangle|\ mod\ p\ \ll x^{7/8-\delta_1}$. By Lemma 5.7 it occurs in at most $O((x^{7/8-\delta_1})^{8/7})=O(x^{1-8/7\delta_1})$ primes $p\leq x$ which is a negligible number relatively to $c_1(\delta_1)\frac{x}{\log^3 x}$ for sufficiently small δ_1.

So, for at most six integers from $a_{i_1},...,a_{i_7},\ q_1(p)$ divides $[\mathbb{F}_p^*:\langle\bar{a_{i_k}}\rangle]$ for $k=1,...,7$. In other words for at most six from $a_{i_1},...,a_{i_7}$ $q_1(p)$ does not divide $|\langle\bar{a}_{i_k}\rangle|$. Hence for at least one integer, say a_n, $q_1(p)$ divide $|\langle\bar{a}_n\rangle|$.

Denote by S_{n-1} the set $\{a_1, ..., a_{n-1}\}$. By repeating the former process for S_{n-1} we obtain that for at least one integer, say a_{n-1}, $q_1(p)$ divide $|\langle \bar{a}_{n-1} \rangle|$.

We continue this process till we obtain the set $T_1 = \{a_7, ..., a_n\}$ where $a_7, ..., a_n$ are multiplicatively independent integers such that $q_1(p)$ divides $|\langle \bar{a}_t \rangle|$ for $t = 7, ..., n$.

By repeating this process for $q_2(p)$ we obtain for the set $T_2 = \{a_{13}, ..., a_n\}$ that $q_2(p)$ divides $|\langle \bar{a}_t \rangle|$ for $t = 13, ..., n$.

Again, by repeating this process for $q_m(p)$ we obtain for the set $T_m = \{a_{6m+1}, ..., a_n\}$ that $q_m(p)$ divides $|\langle \bar{a}_t \rangle$ for $t = 6m + 1, ..., n$.

Since the maximum value of m is 7, if we take $n = 6m + 1 = 43$ multiplicatively independent integers we obtain that one of them have at least the order $\frac{p-1}{d_-}$

Let us look on the algebraic number $M(\alpha)$. By the same method we obtain that one of 43 $M(\alpha)$ have at least the order $\frac{p+1}{d_+}$. one of $42 + 43 = 85$ has, at least, the order $\frac{p^2-1}{24}$. This completes the proof of Theorem 5.1

6. Gcd of exponent functions

As we mentioned, Gupta and Murty's method to attack the former problems raises question regarding $\gcd(a^n - 1, b^n - 1)$ where a, b are multiplicatively independent rational positive integers. We prove a result on the divisors of $\gcd(a^n + 1, b^n + 1)$ which is the same to APR result [3] for $\gcd(a^n - 1, b^n - 1)$.

Theorem 6.1. *Let a and b be two multiplicatively independent integers. Then there exist infinitely many integers n such that*

$$(a^n + 1, b^n + 1) > exp(exp(c \log n / \log\log n))$$

where c is some positive constant.

Since the proof is based on the work of APR we now give the principal proof of this result.

The proof is based on the following simple fact:

Let a be any integer. By the Little Fermat Theorem, if $(a, p) = 1$, where p is a prime number, then

$$a^{p-1} \equiv 1 \ (mod\ p) \quad (or\ p|(a^{p-1} - 1)). \tag{6.1}$$

It is clear that (6.1) is true for all integer n with $p - 1|n$. So, for all integers n with $p - 1|n$ the following holds

$$a^{n} \equiv 1 \ (mod\ p) \quad (or\ p|a^{n} - 1). \tag{6.2}$$

Hence, for finding 'big' divisor of $a^n - 1$ it is enough to find a lot of primes p where $p - 1|n$.

Let K be a square-free positive integer (which will be a product of a "lot" of "small" primes). We want to count the number of integers $m \leq x$ and primes $p \leq x$ such that

$$m(p - 1) \equiv 0 \ (mod\ K) \tag{6.3}$$

Let $\mathbf{A}$ be the number of solutions of the congruence (6.3) where $m \leq x$ and $p \leq x$. To estimate $\mathbf{A}$, for all $d|K$ define the integer $\mathbf{A}_d$ to be the number of solutions of (6.3) where $d|p - 1$ and $(m, K) = K/d$.
Now, we estimate the integer $\mathbf{A}_d$

By APR:

$$|\{p \leq x|p - 1\ square - free\ and\ d|p - 1\}| > \frac{x}{10d \log x}$$

On the other hand,

$$\begin{aligned}&|\{m \leq x|(m,K) = K/d\}|\\ &= |\{m \leq x|(m/(K/d), K/(K/d)) = 1\}|\\ &= |\{m \leq x|(m/(K/d), d) = 1\}| = [\frac{x}{K/d}]\varphi(d) > [x/K]\varphi(d)\end{aligned}$$

Hence

$$\mathbf{A}_d \geq \frac{x}{10d\log x}[x/K]\varphi(d) > \frac{x^2}{20K\log x}\frac{\varphi(d)}{d}$$

We obtain that

$$\mathbf{A} = \sum_{d|K}\mathbf{A}_d > \frac{x^2}{20K\log x}\sum_{d|K}\frac{\varphi(d)}{d} = \frac{x^2}{20K\log x}\prod_{p|K}(2-1/p) \geq \frac{x^2}{20K\log x}(\frac{3}{2})^{\omega(K)}$$

Now, the number of integers $n \leq x^2$ such that $K|n$ is at most x^2/K. Furthermore, each solution, (p,m), represents such n.

Thus there exists some $n \leq x^2$ with $K|n$ which has at least

$$\frac{\mathbf{A}}{x^2/K} > \frac{1}{20\log x}(\frac{3}{2})^{\omega(K)}$$

representations as $m(p-1)$.

Now we can choose (See APR) K to be the product of all the primes till $(1/2)\delta\log x$, possibly without one, where δ is some computable real number, $0 < \delta < 1$.

Hence,

$$\frac{\mathbf{A}}{x^2/K} > \frac{1}{20\log x}(\frac{3}{2})^{\frac{(1/4)\delta\log x}{\log\log x}} \gg exp(\frac{c\log x}{\log\log x})$$

where c is some computable constant.

Now we want to prove the theorem.

Proof. It is clear that if $p-1|n$ we obtain $a^n + 1 \equiv 2\ (mod\ p)$, hence we must modify APR's technique.

On the other hand, if $(\frac{a}{p}) = -1$, $\frac{p-1}{2}|n$ and n is odd we obtain that $a^n + 1 \equiv 0 \ (mod \ p)$ (since n is odd $p-1 \nmid n$). Hence, if $(\frac{a}{p}) = (\frac{b}{p}) = -1$, $\frac{p-1}{2}|n$ but $p-1 \nmid n$ and n is odd we obtain that $p|gcd(a^n+1, b^n+1)$.

We construct such $p's$ in the same way as in the APR's article.

First, we formulate congruence condition such that $(\frac{a}{p}) = (\frac{b}{p}) = -1$ where $\frac{p-1}{2}$ is odd, in other words, where $p \equiv 3 \ (mod \ 4)$.

So, our condition is equivalent to the condition

$$(6.4) \qquad \left(\frac{-1}{p}\right) = \left(\frac{a}{p}\right) = \left(\frac{b}{p}\right) = -1$$

This is equivalent to the condition

$$B(p) = (1 - \left(\frac{-1}{p}\right))(1 - \left(\frac{a}{p}\right))(1 - \left(\frac{b}{p}\right)) =$$
$$1 - \left(\frac{-1}{p}\right) - \left(\frac{a}{p}\right) + \left(\frac{-a}{p}\right) - \left(\frac{b}{p}\right) + \left(\frac{-b}{p}\right) + \left(\frac{ab}{p}\right) - \left(\frac{-ab}{p}\right) \neq 0$$

¿From the fact that for non-perfect square n it is true that

$\sum\limits_{p \leq z} (\frac{n}{p}) = o(\pi(z))$ as $z \to \infty$,

we obtain that $\sum\limits_{p \leq z} (B(p))$ is asymptotic at least to $\pi(z)$. So, for the simultaneous condition 6.4 there are infinitely many solutions p. We fix some p_0 which fulfill's the simultaneous condition and look at all the primes $p \equiv p_0 \ (mod \ 8ab)$.
For such primes,

$(\frac{a}{p}) = (\frac{a}{p_0}) = -1$ and $(\frac{b}{p}) = (\frac{b}{p_0}) = -1$.

In addition it is clear that $p \equiv 3 \ (mod \ 4)$.

Now, consider the congruence

$$m\frac{p-1}{2} \equiv 0 \ (mod\ K) \tag{6.5}$$

with $p \equiv p_0 \ (mod\ 8ab)$, m an odd integer and K a multiple of a lot of small primes. Assume that the divisors of abp_0 do not divide K.

As before, let $\mathbf{A}$ be the number of solutions of the congruence (6.5) where $m \leq x$ and $p \leq x$. For all $d|K$ define $\mathbf{A}_d$ as the number of those solutions where $d|\frac{p-1}{2}$ and $(m, 2K) = K/d$ with $p \equiv p_0 \ (mod\ 8ab)$

Let us estimate $\mathbf{A}_d$. Define

$$\theta_0(x, d, e) = \sum_{\substack{p \leq x \\ p \equiv e \ (mod\ d)}} (\mu(p-1))^2 logp$$

let ψ denote the multiplicative function whose value at the prime power p^r is $\psi(p^r) = \frac{p^2-p}{p^2-p-1}$ and let α denote Artin's constant, $\alpha = \prod_p \frac{p^2-p-1}{p^2-p} = 0.3740$. Note that for all K, $\alpha \leq \alpha\psi(K) < 1$.
By Remark 6.1 in APR's paper, for $d|K$, if $(d, e) = 1$ and $l = (d, e-1)$ then

$$\theta_0(x, d, e) \sim \frac{\alpha\psi(d)\varphi(l)}{\varphi(d)l} x$$

¿From this, if $(d, e) = 1$ and $l = (d, e-1)$

$$\pi_0(x, d, e) := \sum_{\substack{p \leq x \\ p \equiv e \ (mod\ d)}} (\mu(p-1))^2 \geq \frac{1}{\log x}\theta_0(x, d, e)$$
$$\sim \frac{\alpha\psi(d)\varphi(l)}{\varphi(d)l}\frac{x}{\log x} \gg \frac{x}{\varphi(d)\log x}$$

Hence

$$\begin{aligned}&|\{p \leq x|\ d|\frac{p-1}{2}\ \textit{and}\ p \equiv u\ (mod\ 8ab)\}|\\&= |\{p \leq x|\ p \equiv t\ (mod\ 8abd)\}| > \frac{x}{\varphi(8abd)\log x}\end{aligned}$$

On the other hand, if we denote by d' the quotient K/d we have

$$\begin{aligned}|\{m \leq x|(m, 2K) = K/d\}| &= |\{m \leq x|(m/d', 2K/d') = 1\}|\\&= [\frac{x}{K/d}]\varphi(d) > [x/K]\varphi(d)\end{aligned}$$

Hence

$$\mathbf{A}_d \gg \frac{x}{\varphi(8abd)\log x}[x/K]\varphi(d) \gg \frac{x^2}{K\log x}$$

We obtain that

$$\mathbf{A} = \sum_{d|K}\mathbf{A}_d \gg \frac{x^2}{K\log x}\sum_{d|K}1 = \frac{x^2}{K\log x}2^{\omega(K)}$$

Now, the number of integers $n \leq x^2$ such that $2K|n$ is at most $x^2/2K$. Furthermore, each solution (p, m) represents such n.
Thus there exists some $n \leq x^2$ with $K|n$ that has at least

$$\mathbf{A}/\frac{x^2}{K} \gg \frac{2^{\omega(K)}}{\log x}$$

representations as $m(p-1)$.

Now we can choose (See APR) K to be the product of all the primes till $(1/2)\delta\log x$, with the exception of some finite number of primes, where δ is some real number, $0 < \delta < 1$. So, there exists some $n \leq x^2$ with $K|n$ that has at least

$$\mathbf{A}/\frac{x^2}{K} \gg exp(\frac{c'\log x}{log\log x})$$

representations as $m(p-1)$. Where c' is some constant.
By taking the product of all this p's we obtain the result.

□

As we saw the condition for using this method, to find prime divisors of $gcd(a^n+1, b^n+1)$ was that a and b are not perfect squares. But if a and b does perfect squares and there exists natural number s such that $a^{1/2s}, b^{1/2s}$ integers which are not perfect squares, we can use this method to obtain the same result (in the proof, instead of a and b we take $a^{1/2s}$ and $b^{1/2s}$ respectively, and instead of $\frac{p-1}{2}|n$ we take $\frac{p-1}{2^s}|n$)

Also, we note that we can use this method for $gcd(a^n+1, b^n-1)$ and obtain the same result, (instead of the simultaneous condition $(\frac{a}{p}) = (\frac{b}{p}) = -1$ which is suitable to the case $gcd(a^n+1, b^n+1)$, we take $(\frac{a}{p}) = -1$ and $(\frac{b}{p}) = 1$).

7. Application with sieve method

Let $\ell_r(p)$ $(\ell_{nr}(p))$ denote the smallest prime which is quadratic residue (non-residue) *mod* p and $z(x)$ any real unbounded increasing function. In 1965 (See [7]) Erdös proved that there is a set of primes with density one such that $\ell_{nr}(p) < z(p)$. Two years after that Elliot (See [6]) proved this for $\ell_r(p)$. We show this with an elementary method and generalize this result in the sense that the $\ell_r(p)$'s $(\ell_{nr}(p)$'s) can be chosen from a specific infinite set which fulfills a certain condition . Then, we present an interesting application with the proof technique of the result. First, we prove Erdös and Elliot theorems.

Theorem 7.1. *There is a set of primes p with density one such that $\ell_r(p) < z(p)$ (resp. $\ell_{nr}(p) < z(p)$)*

The proof is based on an elementary idea, which will be formulated in Lemma 7.2 and proved in the next section.

Lemma 7.2. *For any odd primes p and q we have :*

(1) $q|p+1,\ p \equiv 3\ (mod\ 4) \Rightarrow (\frac{q}{p}) = 1.$

(2) $q|p-1,\ p \equiv 1\ (mod\ 4) \Rightarrow (\frac{q}{p}) = 1.$

(3) $q|p+1,\ p \equiv 1\ (mod\ 4)$ *and* $q \equiv 3\ (mod\ 4) \Rightarrow (\frac{q}{p}) = -1.$

(4) $q|p-1,\ p \equiv 3\ (mod\ 4)$ *and* $q \equiv 3\ (mod\ 4) \Rightarrow (\frac{q}{p}) = -1.$

So, if we show that there is a set of odd primes p with density one such that for all elements in this set there exists some odd prime $q,\ q < z(p)$ such that $q|p+1$ where $p \equiv 3\ (mod\ 4)$ or $q|p-1$ where $p \equiv 1\ (mod\ 4)$, then we will get that there is a set of primes p with density one such that $\ell_r(p) < z(p)$.

Similarly, if we show that there is a set of odd primes p with density one such that for all elements in this set there exists some odd prime $q,\ q < z(p),\ q \equiv 3\ (mod\ 4)$ such that $q|p+1$ where $p \equiv 1\ (mod\ 4)$ or $q|p-1$ where $p \equiv 3\ (mod\ 4)$, then we get that there is a set of primes p with density one such that $\ell_{nr}(p) < z(p)$

7.1. **Proof of The result.** Let us Start with proof of Lemma 7.2

Proof. If $q|p+1 \Rightarrow p \equiv -1\ (mod\ q) \Rightarrow (\frac{p}{q}) = (\frac{-1}{q}) = (-1)^{\frac{q-1}{2}}$. on the other hand $(\frac{p}{q}) = (\frac{q}{p})(-1)^{\frac{p-1}{2}\frac{q-1}{2}}$. Hence $(\frac{q}{p})(-1)^{\frac{p-1}{2}\frac{q-1}{2}} = (-1)^{\frac{q-1}{2}}$, so

$$q|p+1 \Rightarrow (\frac{q}{p}) = (-1)^{\frac{p+1}{2}\frac{q-1}{2}} \tag{7.1}$$

If $p \equiv 3\ (mod\ 4)$ we have $(\frac{q}{p}) = 1$. On the other hand, if $p \equiv 1\ (mod\ 4)$ and $q \equiv 3\ (mod\ 4)$ we have $(\frac{q}{p}) = -1$.

In the same way we obtain that

$$q|p-1 \Rightarrow (\frac{q}{p}) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}} \tag{7.2}$$

and as before, if $p \equiv 1\ (mod\ 4)$ we have $(\frac{q}{p}) = 1$. In addition, if $p \equiv 3\ (mod\ 4)$ and $q \equiv 3\ (mod\ 4)$ we have $(\frac{q}{p}) = -1$.

¿From equations (7.1) and (7.2) we get trivially the result of Lemma 7.2. □

We will need the next technical lemma.

Lemma 7.3. $\prod\limits_{\substack{p<z \\ p\equiv 1(mod\ 4)}} (1 - \frac{1}{p-1}) \sim \prod\limits_{\substack{p<z \\ p\equiv 3(mod\ 4)}} (1 - \frac{1}{p-1}) \ll \frac{1}{\sqrt{logz}}$

Proof. We prove only the case $p \equiv 1\ (mod\ 4)$. The case $p \equiv 3\ (mod\ 4)$ is similar.

$$\begin{aligned}\prod_{\substack{p<z\\ p\equiv 1(mod\ 4)}} (1-\frac{1}{p-1}) &= exp(\log \prod_{\substack{p<z\\ p\equiv 1(mod\ 4)}} (1-\frac{1}{p-1}))\\ &= exp(\sum_{\substack{p<z\\ p\equiv 1(mod\ 4)}} \log(1-\frac{1}{p-1})) \simeq exp(\sum_{\substack{p<z\\ p\equiv 1(mod\ 4)}} -\frac{1}{p-1})\\ &= exp(-\sum_{\substack{p<z\\ p\equiv 1(mod\ 4)}} \frac{1}{p-1}).\end{aligned}$$

Since

$\frac{1}{p-1} = \frac{1}{p} + \frac{1}{p(p-1)}$

and

$\sum_{\substack{p<z\\ p\equiv 1(mod\ 4)}} \frac{1}{p(p-1)}$ converges

we obtain that

$\prod_{\substack{p<z\\ p\equiv 1(mod\ 4)}} (1-\frac{1}{p-1}) \ll exp(-\sum_{\substack{p<z\\ p\equiv 1(mod\ 4)}} \frac{1}{p}).$

Since (See [11], p.35)

$\sum_{\substack{p<z\\ p\equiv l\ (modk)}} \frac{1}{p} \ll \frac{loglogz}{\varphi(k)},$

we have

$exp(-\sum_{\substack{p<z\\ p\equiv 1(mod\ 4)}} \frac{1}{p}) \ll exp(-\frac{loglogz}{\varphi(4)}) = exp(-\frac{loglogz}{2}) = \frac{1}{\sqrt{logz}}$

□

Let $\Pi(y; d, l)$ be the number of primes $p \leq x$ such that $p \equiv l\ (mod\ d)$, $P_a(z)$ the product of all odd primes up to z and $\equiv a(mod\ 4)$ and $P(z) = P_1(z)P_3(z)$.

Let $A^-(x, z)$ be the set of $p \leq x$ such that $p \equiv 1\ (mod\ 4)$, $gcd(p-1, P(z)) = 1$, $A^+(x, z)$ be the set of $p \leq x$ such that $p \equiv 3\ (mod\ 4)$, $gcd(p+1, P(z)) = 1$, and $A(x, z) = A^-(x, z) \cup A^+(x, z)$.

In a same way let $A_3^-(x, z)$ be the set of $p \leq x$ such that $p \equiv 3\ (mod\ 4)$, $gcd(p-1, P_3(z)) = 1$, $A_3^+(x, z)$ be the set of $p \leq x$ such that $p \equiv 1\ (mod\ 4)$, $gcd(p+1, P_3(z)) = 1$ and $A_3(x, z) = A_3^-(x, z) \cup A_3^+(x, z)$.

The complement of $|A(x, z)|$ is the set of $p \leq x$ such that either $p \equiv 1\ (mod\ 4)$, $gcd(p-1, P(z)) \neq 1$ or $p \equiv 3\ (mod\ 4)$, $gcd(p+1, P(z)) \neq 1$. In other words (by Lemma 7.2) the complement of $|A(x, z)|$ is the set of $p \leq x$ such that there exists a prime $q < z(x)$ $(\frac{q}{p}) = 1$. Hence it is enough to prove that $|A(x, z)|$ is $o(\pi(x))$.

¿From a similar reason, for the non-residue case, it is enough to prove that $|A_3(x, z)|$ is $o(\pi(x))$.

Lemma 7.4. *(1)* $|A^\pm(x, z)| = \sum\limits_{d|P(z)} \mu(d)\pi(x; 4d, \mp 1)$

(2) $|A_3^\pm(x, z)| = \sum\limits_{d|P_3(z)} \mu(d)\pi(x; 4d, l_\pm)$ *where* $l_\pm$ *are some integers* $(l_\pm, 4d) = 1$.

Proof. $|A^-(x, z)| = \sum\limits_{\substack{p<x \\ p\equiv 1\ (mod\ 4)}} \sum\limits_{d|(p-1, P(z))} \mu(d) = \sum\limits_{d|P(z)} \mu(d) \sum\limits_{\substack{p<x \\ p\equiv 1\ (mod\ d) \\ p\equiv 1\ (mod\ 4)}} 1.$

By the Chinese Remainder Theorem

$$|A^-(x, z)| = \sum_{d|P(z)} \mu(d)\pi(x; 4d, 1).$$

In a similar way we obtain that $|A^+(x, z)| = \sum\limits_{d|P(z)} \mu(d)\pi(x; 4d, -1)$. The proof is similar for $|A_3^\pm(x, z)|$.

□

Now, If we restrict $z < (1/2) log \log x$, then we may use that (PNT in progressions)

$\pi(x; q, a) = \frac{Li(x)}{\phi(q)} + O(\frac{x}{\exp(\sqrt{\log x})})$, $\qquad \forall q < (\log x)^{1-\delta}$
to find that
$|A(x, z)| = Li(x) \prod_{2<q\leq z} (1 - \frac{1}{q-1}) + O(2^{\pi(z)} \frac{x}{\exp(c\sqrt{\log x})})$
By Lemma 2.1, The main term is $\ll Li(x)/logz$ and for $z < (1/2) log \log x$ the O-term is still negligible relative to $x/\log x$.

The result for $|A_3(x, z)|$ is the same (just replace the $logz$ by $\sqrt{logz}$ in the main term)

Now, if we take $z = z(X)$ we have that $z(X) < z(p)$ for $p > X$.Take $X = \frac{x}{\log x}$, so, $z(X) < z(p)$ for $p > \frac{x}{\log x}$, but, the number of primes p such that $p \leq \frac{x}{\log x}$ is at most $O(\frac{x}{\log^2 x})$, which have density 0 in the set of all primes.

Note 7.5. If we take $P_a(z)$ to be $P_a(Q, z)$ where $P_a(Q, z)$ is the product of all odd primes q up to z which $\equiv a$ $(mod\ 4)$ and $q \in Q$ and assume that

$$\prod_{\substack{q<z,\ q\in Q \\ q\equiv a\ (mod\ 4)}} (1 - \frac{1}{q-1})$$

is a decreasing function we obtain that $\ell_r(p)$'s ($\ell_{nr}(p)$'s) can be chosen from the infinite set Q.

Note 7.6. In fact, what we obtain from the proof is that we have infinitely many primes p with density 1 such that for any such p there is a prime $q|(P(z), p-1)$. Let a and b be any integers and $P_-(z)$ be $P(z)/ab$. By the same proof we have infinitely many primes p with density 1 such that for any such p there is a prime $q|(P_-(z), p-1)$.

By the Little Fermat Theorem, if $(a, p) = 1$, where p is any prime number, then

$$a^{p-1} \equiv 1 \ (mod \ p) \quad (or \ p|a^{p-1}). \tag{7.3}$$

It is clear that (7.3) is true for all integer n with $p - 1|n$. So, for all integer n with $p - 1|n$ the congruence

$$a^{n} \equiv 1 \ (mod \ p) \quad (or \ p|a^{n} - 1). \tag{7.4}$$

holds. From this it is clear that we can find n such that $P_{-}(z)|a^{n} - 1$ and $P_{-}(z)|b^{n} - 1$ so, $P_{-}(z)|(a^{n} - 1, b^{n} - 1)$. Hence, we obtain infinitely many primes p with density 1 such that for each p there is $q|P_{-}(z)$ such that

$$q|(a^{n} - p, b^{n} - p)$$

References

[1] N. Ailon, Z. Rudnick, *Torsion points on curves and common divisors of* $a^{k} - 1$ *and* $b^{k} - 1$, Acta Arith. 113 (2004), no. 1, 31–38.

[2] E. Artin, *Collected Papers, Reading,* MA:Addison-Wesley (1965).

[3] L. Adleman, C. Pomerance, R. Rumely, *On distinguishing prime numbers from composite numbers*, Ann. of math. (2) 117 (1983), no. 1, 173-206.

[4] Y. Bugeaud, P. Corvaja, U. Zannier, *An upper bound for the GCD of* $a^{n} - 1$ *and* $b^{n} - 1$, Math. Z. 243(2003), no.1. 79-84.

[5] E. Bombieri, *On the large sieve*, Mathematika 12 (1965), 201-225.

[6] Elliot, P.D.T.A. *Some notes on k-th power residues* Acta Arith. 14 1967/1968 153-162.

[7] Erdös, Paul *Remarks on number theory I* Mat Lapok 12 1961 10-17 10.64 (10.42).

[8] G. Cooke and P. J. Wienberger, *On the construction of division chains in algebraic number rings, with applications to* SL_{2}, Comm. Algebra 3 (1975),

481-524.

[9] R. Gupta and R. Murty, *A remark on Artin's conjecture*, Invent. Math. 78, 127-130 (1984).

[10] R. Gupta, V. Kumar Murty and M. Ram Murty, *The Euclidean algorithm for S integers, CNS Conference Proceedings*, Vol.7 (1985), 189-202.

[11] Halberstam and Richert, *Sieve Methods,* Academic Press, London 1974.

[12] D. R. Heath-Brown, Artin's conjecture for primitive roots, Quart. J. Math. Oxford (2), 37 (1986), 27-38.

[13] C. Hooley, *On Artin's Conjecture*, J. Reine Angew. Math. 226 (1967), 209-220.

[14] P. Kurlberg and Z. Rudnick, *Hecke theory and equidistribution for the quantization of linear maps of the torus*, Duke Math. Jour. 103 (2000), 47-77.

[15] P. Kurlberg and Z. Rudnick, *On quantum ergodicity for linear maps of the torus*, Comm. in Math. Physics. 222 (2001) 1, 201-227.

[16] H. W. Lenstra, Jr., *On Artin's conjecture and Euclid's algorithm in global fields*, Invent. Math. 42, (1977), 201-224.

[17] D. Marcus, *Number Fields*, Springer, New York 1977.

[18] W. Narkiewicz, *A note on Artin's conjecture in algebraic number fields*, J. Reine Angew. Math. 381 (1987), 110-115.

[19] W. Narkiewicz, *Units in residue classes*, Arc. Math., Vol. 51, 238-241 (1988)

[20] H. Roskam, *Artin's primitive root conjecture for quadratic fields*, J. Number Theory 81(2000), no 1, 93-109.

[21] O. Taussky, *Introduction into connections betwween algebraic number theory and integral matrices,* Appendix to H. Cohn *A Classical Invitation to Algebraic Numbers and Class Fields,* Springer, New York 1978.