THE QUADRATIC FORM $X^2 + kY^2$

LAWRENCE VU

ABSTRACT. This work introduces an elementary method of counting the number of integral solutions i.e. $(x, y) \in \mathbb{Z}^2$ to the quadratic equation $X^2 + kY^2 = n$ for small values of k, namely $1 \leq k \leq 3$.

1. INTRODUCTION

Our first definition serves as an abbreviation for the whole phrase "a solution in $\mathbb{Z}^2$ to the equation $X^2 + kY^2 = n$". For the entire article, let us fix the assumption that $n > 1$ and $k \geq 1$.

Definition. *A* k-representation *of* n *is a solution* $(x, y) \in \mathbb{Z}^2$ *to the equation*

$$X^2 + kY^2 = n.$$

When dealing with counting problem, the first question we should ask is: "*how to distinguish the objects we wish to count?*" In other words, what is the *characteristic* or *invariant* that uniquely identifies each object? In the next section, I shall answer this question by producing a simple invariant that distinguishes the *k-primitive representations* and henceforth, obtains an invariant for the representations of n.

Definition. *A* k-primitive representation *of* n *is a* k*-representation* (x, y) *of* n *such that* $x, y > 0$ *and* $\gcd(x, y) = 1$.

For the sake of simplicity, let us denote

$$\Gamma_n^k := \{(x, y) | (x, y) \text{ is a } k\text{-primitive representation of } n\} \subset \mathbb{Z}^2$$

The invariant introduces an injection from the set of primitive representations to its co-domain. So naturally, we conjecture that this injection is in fact a bijection. But we shall see that it is difficult to establish such a result and in fact, it is not true. Nevertheless, using numerical experiments, one finds an interesting result and formalize the proof. We shall touch that in section 4.

2. Invariant of primitive representations

First, we need to find a criterion between pairs of primitive representations such that when two primitive representations (x, y) and (x', y') satisfies it, they must be identical i.e. $x = x'$ and $y = y'$. The solution I found is inspired from the famous inequality known as

Theorem (CBS Inequality)**.** *For any real numbers $A, B, C, D \in \mathbb{R}$,*

$$(A^2 + B^2)(C^2 + D^2) \geq (AC + BD)^2$$

Equality occurs if and only if $\frac{A}{C} = \frac{B}{D}$ or equivalently $AD - BC = 0$.

Proof. We have an equality

$$(\Diamond) \qquad (A^2 + B^2)(C^2 + D^2) = (AC + BD)^2 + (AD - BC)^2$$

and since $(AD-BC)^2 \geq 0$, the RHS above (and so the LHS) is at least $(AC+BD)^2$. Evidently, equality occurs if and only if $AD-BC = 0$. □

Lemma (Criterion for identical primitive representations)**.** *Two k-primitive representations (x, y) and (x', y') of n are identical if and only if*

$$xy' - x'y = 0.$$

Proof. The forward implication is trivial: if $(x, y) = (x', y')$ then clearly $xy' - x'y = 0$.

For the backward implication, notice that $x', y' > 0$. So the equation $xy' - x'y = 0$ implies

$$\frac{x}{x'} = \frac{y}{y'}$$

and thus, properties of ratios give us

$$\frac{x^2}{x'^2} = \frac{ky^2}{ky'^2} = \frac{x^2 + ky^2}{x'^2 + ky'^2} = \frac{n}{n} = 1.$$

From this, one easily obtains $x = x'$ and $y = y'$. □

Remark: From the proof, the result holds as long as one of the representation does not contain 0 in both coordinates. In particular, when n is not a square, it holds for all representations, not just primitive ones.

The criterion lemma gives an invariant for primitive representations, namely the quotient $\frac{x}{y} \in \mathbb{Q}$. But this invariant is difficult to use because $\mathbb{Q}$ is infinite while we know that Γ_n^k is finite. To transform the infinite to finite, we take the ratio modulo n as in:

Lemma (Invariant for primitive representations)**.** *Two k-primitive representations (x, y) and (x', y') of n are identical if and only if*

$$\frac{x}{y} \equiv \frac{x'}{y'} \pmod{n}$$

Note: For any $(x, y) \in \Gamma_n^k$, $\gcd(x, y) = 1$ so that

$$\begin{aligned} \gcd(y, n) &= \gcd(y, x^2 + ky^2) \\ &= \gcd(y, x^2) \\ &= 1 \end{aligned}$$

so that y is an invertible element of $\mathbb{Z}/n\mathbb{Z}$ and hence, it makes sense to write $\frac{x}{y}$.

Proof. Again, the forward implication is trivial. For the reverse direction, we apply the CBS inequality to get

$$\begin{aligned} n^2 &= (x^2 + ky^2)(x'^2 + ky'^2) \\ &\geq (x^2 + y^2)(x'^2 + y'^2) \qquad \text{as } k \geq 1 \\ &\geq (x^2 + y^2)(y'^2 + (-x')^2) \\ &\geq (xy' - yx')^2 \end{aligned}$$

and hence,

$$|xy' - yx'| \leq n.$$

Notice that equality cannot occurs because $\frac{x}{y'} > 0 > \frac{y}{-x'}$. This forces $-n < xy' - yx' < n$.

So if we assume

$$\frac{x}{y} \equiv \frac{x'}{y'} \pmod{n},$$

then

$$xy' \equiv yx' \pmod{n}$$

or $n|xy' - yx'$. From this divisibility relationship together with the obtained range for $xy' - yx'$ above ($-n < xy' - yx' < n$), we conclude $xy' - yx' = 0$. Now, this reverse implication follows from the earlier lemma. □

The meaning of the lemma is that: each primitive representation is characterized by the congruence class for the ratio of the coordinates. What about general representations? Well, we simply add the information on the $\gcd(x, y)$ and the signs of x and y. Our goal of this section is accomplished.

3. Upper bound for $|\mathbf{\Gamma_n^k}|$

The invariant provided in section 2 gives us an injection

$$\begin{aligned}\gamma : \qquad \Gamma_n^k &\to \mathbb{Z}/n\mathbb{Z} \\ (x,y) &\mapsto \left[xy^{-1} \pmod n\right]\end{aligned}$$

So we must have

$$|\Gamma_n^k| = |\mathrm{Im}(\gamma)| = |\gamma(\Gamma_n^k)|$$

which means the task of counting $|\Gamma_n^k|$ is tantamount to counting the images of γ i.e. find out all the $r \in \mathbb{Z}/n\mathbb{Z}$ such that there exists $(x,y) \in \Gamma_n^k$ with $\gamma((x,y)) = r$.

However, this task is hard; and we shall walk arround it by estimating its range. And this section gives an upper bound for appropriate values of n.

Observe that for any $(x,y) \in \Gamma_n^k$, the ratio $r = \frac{x}{y}$ must be a solution of

$$r^2 + k \equiv 0 \pmod n.$$

As a result:

$$\gamma(\Gamma_n^k) \subseteq R_n^k$$

where

$$R_n^k := \{[r] : r^2 \equiv -k \pmod n\},$$

the set of square-roots of $[-k]$ in the ring $\mathbb{Z}/n\mathbb{Z}$.

From the inclusion, it is tempted to try to prove that $\gamma(\Gamma_n^k) = R_n^k$. Yet, numerical experiments show that it is not always true that every element of $R_{k,n}$ has a pre-image; but typically half of it. Indeed, with a bit more analysis, we have the following result:

Lemma. *When $k > 1$, if $r \in \gamma(\Gamma_n^k)$ then $-r \notin \gamma(\Gamma_n^k)$. When $k = 1$, if $\gamma((x,y)) = r$ then $\gamma((x',y')) = -r$ if and only if $(x',y') = (y,x)$.*

Note: if $r \in R_n^k$ then $-r \in R_n^k$. Also, $r = -r$ if and only if $2r \equiv 0 \pmod n$.

Proof. Suppose that for some $r \in R_{k,n}$ such that there exists $(x,y), (x',y') \in \Gamma_n^k$ such that $\Gamma((x,y)) = \frac{x}{y} = r$ and $\Gamma((x',y')) = \frac{x'}{y'} = -r$.

Then it follows that $xy' \equiv -x'y \pmod n$ or $n | xy' + x'y$. Again, CBS inequality gives us

$$\begin{aligned}0 < xy' + x'y &\le (x^2 + y^2)(y'^2 + x'^2) \\ &\le (x^2 + ky^2)(x'^2 + ky'^2) \\ &\le n\end{aligned}$$

so that $n|xy' + x'y$ forces $xy' + x'y = n$. But then equality must hold throughout: $k = 1$ and the equality in application of CBS inequality must holds. The later happens if and only if $\frac{x}{y'} = \frac{x'}{y}$ or equivalently $xy = x'y'$. So, if $k > 1$, we derive a contradiction, and so r and $-r$ cannot cobelong to the image of Γ.

Now we have a system of equations:

$$\begin{cases} x^2 + y^2 = x'^2 + y'^2 \\ x^2y^2 = x'^2y'^2 \end{cases}$$

And Viete's theorem tells us that (x', y') is either (x, y) or (y, x) given that $x, y, x', y' > 0$. If $(x', y') = (y, x)$ then we are in the conclusion of the lemma. Otherwise, if $(x', y') = (x, y)$ then $xy' + x'y = 2xy = n = x^2 + y^2$. AM-GM inequality implies $x = y$. But since $\gcd(x, y) = 1$, we must have $x = y = 1$ and $n = 2$. In such case, it is still true that $(x', y') = (x, y)$. □

A simple corollary of the lemma and the above discussion is

Corollary. *If $k > 1$ then*

$$|\Gamma_n^k| \leq \frac{1}{2}|R_n^k|.$$

If $k = 1$ and $n > 2$ then

$$|\Gamma_n^k| \leq |R_n^k|.$$

(To be exhaustive, if $k = 1$ and $0 < n \leq 2$ then $|\Gamma_n^k| = n - 1$.)

It remains to compute the number of roots i.e. $|R_n^k|$ to establish an (explicit i.e. in terms of n and k) upper bound for $|\Gamma_n^k|$.

Let $n = \prod_{i=1}^t p_i^{v_i}$ be the standard prime factorization of n. Chinese Remainder Theorem shows that

$$\mathbb{Z}/n\mathbb{Z} \cong \prod_{i=1}^t \mathbb{Z}/p_i^{v_i}\mathbb{Z}$$

so that each solution $r \in \mathbb{Z}/n\mathbb{Z}$ for $r^2 \equiv -k \pmod{n}$ corresponds to a unique $(r_1, r_2, ..., r_t)$ with $r_i \in \mathbb{Z}/p_i^{v_i}\mathbb{Z}$ for all i satisfying

$$r_i^2 \equiv -k \pmod{p_i^{v_i}}.$$

Therefore, we must have

$$|R_n^k| = \prod_{i=1}^t |R_{p_i^{v_i}}^k|.$$

The problem now becomes counting square root of $-k$ modulo prime powers p^v. The next two lemmas complete these computations.

Lemma. *Let p is an odd prime. The number of square roots of $-k = -p^h k'$ modulo p^v (where $p \nmid k'$) i.e. $|R^k_{p^v}|$ is*

(i) *$p^{v-\lceil v/2 \rceil}$ if $h \geq v$;*
(ii) *two if $0 \leq h < v$ and h is even and $\left(\frac{-k'}{p}\right) = 1$;*
(iii) *zero otherwise.*

Proof. Suppose that r is a square root of $-k$.

(i) If $h \geq v$ then

$$r^2 \equiv -k \equiv -p^h k' \equiv 0 \pmod{p^v}$$

Then r is a square root if and only if it is divisible by $p^{\lceil v/2 \rceil}$. In modulo p^v, we have $p^{\lceil v/2 \rceil}, 2p^{\lceil v/2 \rceil}, ..., p^v$. There are thus $p^{v-\lceil v/2 \rceil}$ roots.

(ii) If $0 \leq h < v$ then

$$r^2 \equiv -k \equiv -p^h k' \pmod{p^v}$$

implies

$$r^2 \equiv 0 \pmod{p^h}.$$

Thus, r is divisible by $p^{\lceil h/2 \rceil}$ (by unique factorization). Let $r = p^{\lceil h/2 \rceil} r'$ for $r' \in \mathbb{Z}$ and we obtain

$$p^{2\lceil h/2 \rceil} r'^2 \equiv -p^h k' \pmod{p^v}$$

which is equivalent to

$$p^{2\lceil h/2 \rceil - h} r'^2 \equiv -k' \pmod{p^{v-h}}$$

Note that since $v > h$, p^{v-h} is divisible by p. If $2\lceil h/2 \rceil - h \geq 1$ then $p| - k'$ but this is a contradiction to the hypothesis. Therefore, in order that a square root exists, we must have h being even. In such case, each square root r of $-k$ modulo p^v corresponds to a square root r' of $-k'$ modulo p^{v-h}. From the discussion of quadratic residue, it follows that there are exactly two square roots if $\left(\frac{-k'}{p}\right) = 1$ and no root, otherwise. We are done.

(iii) Follows from the earlier cases.

□

Lemma. *If n is odd and $d := \gcd(n, k)$ is a perfect square then*

$$\Gamma^k_n = \Gamma^{k/d}_{n/d}.$$

Theorem (Upper bound for number of primitive representations)**.** *Suppose that* $\gcd(n, 2k) = 1$ *i.e. n is odd and has no common prime factor with k. Let* $n = \prod_{i=1}^{t} p_i^{v_i} q$ *where* $p_i \nmid k$ *and* $\left(\frac{-k}{p_i}\right) = 1$ *and* $t \geq 1$*. Then*

(i) *if* $q = 1$ *and* $k > 1$*:*

$$|\Gamma_n^k| \leq 2^{t-1}$$

(ii) *if* $q = 1$ *and* $k = 1$*:*

$$|\Gamma_n^k| \leq 2^t$$

(iii) *otherwise:*

$$|\Gamma_n^k| = 0$$

Proof. Follows from the earlier discussion: Let's consider the case when $k > 1$. If $q > 1$ then n contains some prime power p^s such that $|R_{p^s}^k| = 0$ and hence $|R_n^k| = 0$ so $|\Gamma_n^k| = 0$. Otherwise ($q = 1$), $|R_n^k| = \prod_{i=1}^{t} |R_{p_i^{v_i}}^k| = \prod_{i=1}^{t} 2 = 2^t$ and that $|\Gamma_n^k| \leq \frac{1}{2}|R_n^k| = 2^{t-1}$. (Note that $t \geq 1$ implies n must contains an odd prime factor so $n > 2$.) □

Although the last result is only applicable to appropriate values of n and k, in practice we can usually deal with the common factor of n and k separately. Note that it is possible to consider even values of n as well as we can also count square root modulo 2^v, but the result is much less applicable due to exceptional cases.

4. Enumeration of primitive representations

Having obtained the upper bound on the number of primitive representations, we now want to get a lower bound of $|\Gamma_n^k|$. To do so, we need a way to enumerate a class of elements of Γ_n^k.

The idea is simple: utilizing the equation ($\Diamond$) we obtain

$$(\Diamond\Diamond) \qquad (X^2 + kY^2)(Z^2 + kT^2) = (XZ \mp kYT)^2 + k(XT \pm YZ)^2$$

Such an equation gives a way to obtain k-representation for a product $n = ab$ once we have some k-representations for its factor. But in the process of forming these k-representations, we might encounter repetition. So now we ask a similar question: *how do we distinguish different generated representations?* The answer comes in the next result.

Lemma (Criterion for distinct generated representations)**.** *Assume that* $n, n' \in \mathbb{N}_{>0}$ *such that* $\gcd(n, n') = 1$*. Let*

$$(x, y), (x', y') \in \Gamma_n$$
$$(a, b), (a', b') \in \Gamma_{n'}^k$$
$$\varepsilon, \varepsilon' \in \{\pm 1\}$$

be such that $(x', y') \neq (x, y)$*. Then*

$$(|xa - \varepsilon kyb|, |xb + \varepsilon ya|)$$

and

$$(|x'a' - \varepsilon' ky'b'|, |x'b' + \varepsilon' y'a'|)$$

are two distinct primitive representations of nn' *except for the symmetric case when* $k = 1$ *and* $\varepsilon = \varepsilon'$ *and* $(x', y') = (y, x)$ *and* $(a', b') = (b, a)$*.*

Proof. From the equation $(\Diamond\Diamond)$, the two pairs are representations of nn'. We verify that they are indeed primitive.

Let $d = \gcd(|xa - \varepsilon kyb|, |xb + \varepsilon ya|) = \gcd(xa - \varepsilon kyb, xb + \varepsilon ya)$. Then

$$d \mid xa - \varepsilon kyb \quad \text{and} \quad d \mid xb + \varepsilon ya.$$

So we must have

$$d \mid (xa - \varepsilon kyb)a + kb(xb + \varepsilon ya) = x(a^2 + kb^2) = xm$$
$$d \mid (xa - \varepsilon kyb)(-\varepsilon b) + \varepsilon a(xb + \varepsilon ya) = y(a^2 + kb^2) = ym$$

and hence $d \mid \gcd(xm, ym) = m \gcd(x, y) = m$ which is due to the fact that (x, y) is primitive. By symmetry, one also obtains $d \mid \gcd(an, bn) = n \gcd(a, b) = n$. Then $d \mid \gcd(n, m) = 1$ by our assumption. So $d = 1$.

Now if either $|xa - \varepsilon kyb|$ or $|xb + \varepsilon ya|$ is 0, the remaining must be 1 in order that their greatest common divisor is 1. So either $nn' = 1$ or $nn' = k$ and so $n \leq k$. But this is not possible unless $k \geq n = x^2 + ky^2 \geq 1^2 + k \times 1^2 \geq 1 + k$ i.e. $k \geq k + 1$. So, both components are positive.

This shows that $(|xa - \varepsilon kyb|, |xb + \varepsilon ya|)$ (and by symmetry, $(|x'a' - \varepsilon' ky'b'|, |x'b' + \varepsilon' y'a'|)$) are indeed primitive representations of nn'.

It remains to show the distinction between them. By the criterion lemma, the two representations are identical if and only if

$$|xa - \varepsilon kyb| \times |x'b' + \varepsilon' y'a'| - |x'a' - \varepsilon' ky'b'| \times |xb + \varepsilon ya| = 0$$

or equivalently

$$(xa - \varepsilon kyb)(x'b' + \varepsilon' y'a') \pm (x'a' - \varepsilon' ky'b')(xb + \varepsilon ya) = 0$$

where the sign $\pm$ is taken to be $+$ if the two terms are of the different sign and $-$ otherwise.

Let us expand the equations simultaneously and re-arrange the terms:

$$\begin{aligned}
& (xa - \varepsilon kyb)(x'b' + \varepsilon' y'a') \pm (x'a' - \varepsilon' ky'b')(xb + \varepsilon ya) \\
= \; & xx'ab' + \varepsilon' xy'aa' - \varepsilon kyx'bb' - \varepsilon\varepsilon' kyy'ba' \\
& \qquad \pm (xx'ba' + \varepsilon yx'aa' - \varepsilon' kxy'bb' - \varepsilon\varepsilon' kyy'ab') \\
= \; & xx'ab' + \varepsilon' xy'aa' - \varepsilon kyx'bb' - \varepsilon\varepsilon' kyy'ba' \pm xx'ba' \\
& \qquad \pm \varepsilon yx'aa' \mp \varepsilon' kxy'bb' \mp \varepsilon\varepsilon' kyy'ab' \\
= \; & xx'(ab' \pm ba') + \varepsilon' xy'(aa' \mp kbb') + \varepsilon yx'(-kbb' \pm aa') \\
& \qquad + \varepsilon\varepsilon' kyy'(-ba' \mp ab') \\
= \; & xx'(ab' \pm ba') + \varepsilon' xy'(aa' \mp kbb') \pm \varepsilon yx'(\mp kbb' + aa') \\
& \qquad \mp \varepsilon\varepsilon' kyy'(\pm ba' + ab') \\
= \; & (xx' \mp \varepsilon\varepsilon' kyy')(ab' \pm ba') + (\varepsilon' xy' \pm \varepsilon yx')(aa' \mp kbb')
\end{aligned}$$

Let us denote

$$\begin{aligned}
M &:= xx' \mp \varepsilon\varepsilon' kyy' \\
N &:= \varepsilon' xy' \pm \varepsilon yx' \\
P &:= aa' \mp kbb' \\
Q &:= ab' \pm ba'
\end{aligned}$$

then $M, N, P, Q \in \mathbb{Z}$ and we also observe that the following three equations

$$\begin{cases}
MQ + NP = 0 \\
M^2 + kN^2 = n^2 \\
P^2 + kQ^2 = n'^2
\end{cases}$$

holds in both possibilities of the sign. Then we derive

$$\begin{cases}
(MQ)^2 = (NP)^2 \\
(MQ)^2 + k(NQ)^2 = (nQ)^2 \\
(NP)^2 + k(NQ)^2 = (Nn')^2
\end{cases}$$

But then $(MQ)^2 + k(NQ)^2 = (NP)^2 + k(NQ)^2$ so that $(nQ)^2 = (Nn')^2$. Taking the square root of both sides, we obtain

$$n|Q| = |N|n'$$

Now, recall our hypothesis that n and n' are coprime. So the fact that n divides $|N|n'$, suggested from the above identity, forces n to be

a divisor of $|N|$. Again, using CBS inequality, we should have

$$\begin{aligned} N^2 &= (\varepsilon' xy' \pm \varepsilon yx')^2 \\ &= ((\varepsilon' x)y' + (\pm\varepsilon y)x')^2 \\ &\leq ((\varepsilon' x)^2 + (\pm\varepsilon y)^2)(x'^2 + y'^2) \\ &= (x^2 + y^2)(x'^2 + y'^2) \\ &\leq (x^2 + ky^2)(x'^2 + ky'^2) \\ &= n^2 \end{aligned}$$

So $0 \leq |N| \leq n$. Now, the earlier conclusion that $|N|$ is divisible by n implies either $|N| = 0$ or $|N| = n$. Now we consider two cases:

- $|N| = n$
  Then the equation $M^2 + kN^2 = n^2$ forces $k = 1$ and $M = 0$ or $xx' \mp \varepsilon\varepsilon' kyy' = 0$ so that the sign $\mp$ must be that of $-\varepsilon\varepsilon'$ so that we get $xx' - yy' = 0$; otherwise, we should get $xx' + yy' = 0$ which is absurd as $x, x', y, y' > 0$. Note that as $k = 1$, (y, x) is also a primitive representation. Applying the identical criterion lemma with (y, x) and (x', y'), we should get $(x', y') = (y, x)$. By symmetry, we also have $|Q| = n'$ and similar reasoning gives $(a', b') = (b, a)$. Now, it is easy to see that $\varepsilon = \varepsilon'$.
- $|N| = 0$
  Then we deduce $N = 0$ or $\varepsilon' xy' \pm \varepsilon yx' = 0$ or $xy' \pm \varepsilon\varepsilon' yx' = 0$. Again, the sign $\pm$ must be that of $-\varepsilon\varepsilon'$ or we get the same contradiction. But then $xy' - yx' = 0$ which means $(x', y') = (x, y)$ due to identical criterion lemma. This contradicts our hypothesis about the distinction between (x', y') and (x, y).

□

The lemma gives us a mean to enumerate a class of primitive representations. For example, from $5 = 2^2 + 1^2 = 1^2 + 2^2$ and $13 = 3^2 + 2^2 = 2^2 + 3^2$, one obtains

$$\begin{aligned} 5 \times 13 &= 4^2 + 7^2 \\ &= 7^2 + 4^2 \\ &= 1^2 + 8^2 \\ &= 8^2 + 1^2 \end{aligned}$$

Theorem (Lower bound for number of primitive representations)**.** *Let* $n = \prod_{i=1}^{t} p_i^{v_i}$ *for* $t \geq 1$*. Then*

$$|\Gamma_n^k| \geq 2^{t-1} \prod_{i=1}^{t} |\Gamma_{p_i^{v_i}}^k|$$

if $k > 1$ *and*

$$|\Gamma_n^k| \geq \prod_{i=1}^{t} |\Gamma_{p_i^{v_i}}^k|$$

if $k = 1$*.*

Proof. By induction on t, the number of prime factors of n. We shall only prove the case $k > 1$, leaving the other (more tricky) case to the reader.

- Base case $t = 1$: Then $n = p_1^{v_1}$

  $$LHS = |\Gamma_n^k|$$
  $$RHS = 2^{t-1}|\Gamma_{p_1^{v_1}}^k| = |\Gamma_n^k|$$

  so we have the equality.
- Induction: Suppose that the inequality holds for $t - 1$ i.e.

  $$|G| \geq 2^{t-2} \prod_{i=1}^{t-1} |\Gamma_{p_i^{v_i}}|$$

  where $G = \Gamma^k_{\prod_{i=1}^{t-1} p_i^{v_i}}$.

  Then for any $(x, y) \in G$ and any $(a, b) \in \Gamma_{p_t^{v_t}}$ and any $\varepsilon \in \{\pm 1\}$, one obtains an element of Γ_n^k. Due to the criterion for distinct generated representations lemma, these elements must be distinct because $k > 1$. Hence, the number of elements in Γ_n^k is at least the product of

  $$|G| \times |\Gamma_{p_t^{v_t}}| \times |\{\pm 1\}|$$

  which is bounded below by

  $$2^{t-2} \prod_{i=1}^{t-1} |\Gamma_{p_i^{v_i}}| \times |\Gamma_{p_t^{v_t}}| \times 2$$

  by induction hypothesis, or equally by

  $$2^{t-1} \prod_{i=1}^{t} |\Gamma_{p_i^{v_i}}|.$$

  Thus, we established the inductive case. By mathematical induction, we get the theorem.

□

As a remark, this result does not place any constraint on n unlike its upper bound counter-part. However, it is only useful when there is no prime power $p_i^{v_i}||n$ that has no primitive representations; because if there is, then the right hand side is 0 so the theorem only says $|\Gamma_n^k| \geq 0$ which is a tautology.

In case every prime power $p_i^{v_i}$ exactly divides n has a representation, we derive some useful information. And we state it in the next theorem.

Theorem. *Let* $n = \prod_{i=1}^{t} p_i^{v_i}$ *be such that* $\gcd(n, 2k) = 1$ *and all* $p_i^{v_i}$ *has a primitive representation. Then if* $k > 1$ *then*

$$|\Gamma_n^k| = 2^{t-1}$$

and if $k = 1$ *then*

$$|\Gamma_n^k| = 2^t$$

Proof. We prove the theorem only the case when $k > 1$. The case $k = 1$ is analogous.

Since $p_i^{v_i}$ has a primitive representation, it follows that

$$\left(\frac{-k}{p_i}\right) = 1$$

and

$$|\Gamma_{p_i^{v_i}}| \geq 1$$

so that the upper bound and lower bound theorems give

$$2^{t-1} \leq 2^{t-1} \prod_{i=1}^{t} |\Gamma_{p_i^{v_i}}| \leq |\Gamma_n^k| \leq 2^{t-1}.$$

Thus, equality must hold throughout and we derive:

$$|\Gamma_{p_i^{v_i}}| = 1$$

for all $i = 1, 2, ..., t$ and that

$$\Gamma_n^k = 2^{t-1}$$

□

Corollary. *Let* p *be a prime such that* $p > 2$ *and* $p \nmid k$ *and* p^v *has a primitive representation. Then either that representation is the unique primitive representation of* p^v *(if* $k > 1$*) or* p^v *has exactly two symmetric representations.*

5. Representations counting theorems

Our final target of this exposition is to count the number of primitive and general representations.

Unfortunately, it is not currently possible to provide a general theorem that work for all quadratic forms $X^2 + kY^2$. But we can do so for small values of k, namely $k = 1, 2, 3$.

Theorem (Fermat-Euler)**.** *For every odd prime p such that $p \nmid k$ and $\left(\frac{-k}{p}\right) = 1$, p^t has a unique primitive representation when $k > 1$ and has two symmetric primitive representations when $k = 1$.*

Proof. Omitted. □

Theorem (Counting theorem for $k = 1$)**.** *Let n be factorized into $2^s \prod_{i=1}^{t} p_i^{v_i} \prod_{j=1}^{l} q_j^{u_j}$ where $p_i \equiv 1 \pmod 4$ and $q_j \equiv -1 \pmod 4$.*

(i) *The number of primitive representations of n is 2^t if $s \leq 1$ and $u_j = 0$ for all $j = 1, 2, ..., l$; and is 0 otherwise.*

(ii) *The number of representations of n is $4 \prod_{i=1}^{t} (v_i + 1)$ if q_j are all even; and is 0 otherwise.*

Theorem (Counting theorem for $k = 2$)**.** *Let n be factorized into $2^s \prod_{i=1}^{t} p_i^{v_i} \prod_{j=1}^{l} q_j^{u_j}$ where $p_i \equiv 1, 5 \pmod 8$ and $q_j \equiv 3, 7 \pmod 8$.*

(i) *The number of primitive representations of n is 2^{t-1} if $0 \leq s \leq 1$ and $u_j = 0$ for all $j = 1, 2, ..., l$; and is 0 otherwise.*

(ii) *The number of representations of n is $2 \prod_{i=1}^{t} (v_i + 1)$ if q_j are all even; and is 0 otherwise.*

Theorem (Counting theorem for $k = 3$)**.** *Let n be factorized into $2^s 3^r \prod_{i=1}^{t} p_i^{v_i} \prod_{j=1}^{l} q_j^{u_j}$ where $p_i \equiv 1 \pmod 3$ and $q_j \equiv -1 \pmod 3$.*

(i) *The number of primitive representations of n is $2^{t+\frac{s}{2}-1}$ if $s = 0$ or $s = 2$ and $0 \leq r \leq 1$ and $u_j = 0$ for all $j = 1, 2, ..., l$; and is 0 otherwise.*

(ii) *The number of representations of n is $2 \prod_{i=1}^{t} (v_i + 1)$ if s is even and q_j are all even; and is 0 otherwise.*

6. Conclusion