Sum of three squares and class numbers of imaginary quadratic fields

By Peter Jaehyun CHO

Department of Mathematics, University of Toronto, Bahen Centre,
40 St. George St., Toronto, Ontario, Canada, M5S 2E4

(Communicated by Shigefumi MORI, M.J.A., May 12, 2011)

Abstract: For a positive integer k and a certain arithmetic progression A, there exist infinitely many quadratic fields $\mathbf{Q}(\sqrt{-d})$ whose class numbers are divisible by k and $d \in A$. From this, we have a linear congruence of the representation numbers of integers as sums of three squares.

Key words: Sum of three squares; class number; imaginary quadratic field; arithmetic progression.

1. Introduction. Let $r(n)$ be the representation numbers of integers as sum of three squares. Then $r(n)$ are Fourier coefficients of weight $\frac{3}{2}$ modular form $\theta_0(z)^3$ of $\Gamma_0(4)$.

$$\begin{aligned}\textstyle\sum_{n=0}^{\infty} r(n)q^n &:= \theta_0(z)^3 \\ &= 1 + 6q + 12q^2 + 8q^3 + 6q^4 + 24q^5 + \cdots.\end{aligned}$$

Gauss showed that $r(n)$ is a multiple of Hurwitz-Kronecker class number.

$$r(n) = \begin{cases} 12H(4n) & \text{if } n \equiv 1, 2 \mod 4 \\ 24H(n) & \text{if } n \equiv 3 \mod 8 \\ r(n/4) & \text{if } n \equiv 0 \mod 4 \\ 0 & \text{if } n \equiv 7 \mod 8. \end{cases}$$

If $-N = Df^2$ where D is a negative fundamental discriminant, then $H(N)$ is given by class number $h(D)$ of imaginary quadratic field $\mathbf{Q}(\sqrt{D})$.

$$H(N) = \frac{h(D)}{w(D)} \sum_{d|f} \mu(d) \left(\frac{D}{d}\right) \sigma_1\left(\frac{f}{d}\right)$$

where $w(D)$ is half of the number of units in $\mathbf{Q}(\sqrt{D})$ and $\sigma_1(n)$ is the sum of the positive divisors of n. Hence divisibility of $r(n)$ is equivalent to divisibility of class numbers of imaginary quadratic fields. Kohnen and Ono [2] showed indivisibility of class numbers of imaginary quadratic fields by prime numbers in an ingenious way under this observation. Nagell [4], Ankeny and Chowla [1], Kuroda [3], Soundararajan [6] and many other mathematicians showed that for given integer k, there are infinitely many imaginary quadratic fields $\mathbf{Q}(\sqrt{-d})$ whose class numbers are divisible by k. Especially in Ankeny and Chowla [1], $-d$ is always congruent to 3 modulo 4, this implies that for given k, there exist infinitely many square-free integers n such that $n \equiv 1 \mod 4$ and $r(n) \equiv 0 \mod 12k$.

From these observations, we are motivated to study divisibility problem of class numbers of imaginary quadratic fields with discriminants in an arithmetic progression.

For an odd positive square-free integer M and an integer a, we define an arithmetic progression $A(a, M)$ be

$$A(a, M) = \{n \in \mathbf{Z} \mid n \equiv a \mod M\}.$$

Throughout this article, we assume that for a given prime number p, p and M are co-prime or M is divided by p with order 1. So M is factorized into $p_1 p_2 \cdots p_s$ for the former case and into $pp_1 p_2 \cdots p_s$ for the latter case.

Now we can state two main theorems in this article.

Theorem 1. *Let k be a positive integer and m be a quadratic residue modulo M. Let p be an odd prime number bigger than 3 with $c(p, M) > 0$ where* $c(p, M) = \left(\frac{9}{4} - \frac{\pi^2}{6} + \frac{1}{p^2} + \sum_{i=1}^{s}\left(\frac{1}{p_i^2} - \frac{1}{p_i}\right)\right)$.

If $p \mid M$, we assume that m is a non-zero quadratic residue modulo M and modulo p simultaneously. Then, there are infinitely many positive square-free d such that

$$h(-d) \equiv 0 \mod k \text{ and } -d \in A(m - p^k, M)$$

where $h(-d)$ is the class number of imaginary quadratic field $\mathbf{Q}(\sqrt{-d})$.

2010 Mathematics Subject Classification. Primary 11R11, 11R29.

doi: 10.3792/pjaa.87.91

From Ankeny and Chowla [1] and the argument of the proof of Theorem 1, we have a linear congruence property of $r(n)$.

Theorem 2. *Let $r(n)$ be the representation numbers of integers as sum of three squares. Then,*
1) *For any given integer k, there are infinitely many square-free n such that*

$$n \equiv 1 \mod 4 \text{ and } r(n) \equiv 0 \mod 12k.$$

2) *For any given odd integer k, there are infinitely many square-free n such that*

$$n \equiv 2 \mod 4 \text{ and } r(n) \equiv 0 \mod 12k.$$

3) *For any given odd integer k, there are infinitely many square-free n such that*

$$n \equiv 3 \mod 8 \text{ and } r(n) \equiv 0 \mod 24k.$$

Remark 1. We can state Theorem 1 and Theorem 2 in more quantitative way. For example, proof of Theorem 1 implies $|\{0 < n < X \mid n : \text{square-free}, \ n \equiv 1 \mod 4 \text{ and } r(n) \equiv 0 \mod 12k\}| \gg X^{1/2}$.

We will prove Theorem 1 and its corollary in section 2 and prove Theorem 2 in section 3.

2. Proof of Theorem 1. We clearly mention that main ideas of proofs in this article comes from Ankeny and Chowla [1]. To prove above Theorem 1, we need the following two Lemmas. In this section, we assume that k is sufficiently large.

Lemma 3. *Let $N(k,p,r,M)$ be the number of the square free integers $d = p^k - l^2$, such that l is even, $l \equiv r$ mod M and $0 < l < \sqrt{(p-4)p^{k-1}}$.*

If $p \mid M$, we assume that r is a non-zero residue modulo M and modulo p simultaneously. Then we have

$$N(k,p,r,M) > \widetilde{c}(p,M)\sqrt{(p-4)p^{k-1}}.$$

$$\text{where } \widetilde{c}(p,M) = \begin{cases} \frac{(p-1)c(p,M)}{2pM} & \text{if } p \nmid M \\ \frac{c(p,M)}{2M} & \text{if } p \mid M. \end{cases}$$

Proof. First, we assume that p and M are coprime. We define $S(k,p,r,a,M) := \{p^k - l^2 \mid l : \text{even}, \ l \equiv r \mod M, \ l \equiv a \mod p \text{ and } 0 < l < \sqrt{(p-4)p^{k-1}}\}$ where a is any nonzero residue modulo p. Then we obtain that

$$|S(k,p,r,a,M)| = \frac{\sqrt{(p-4)p^{k-1}}}{2pM} + O(1).$$

Then any d in $S(k,p,r,M)$ is not divisible by p^2. We exclude d such that ${p_1}^2 \mid d$ from $S(k,p,r,a,M)$ where p_1 is a prime divisor of M. Let m_1 be the smallest integer such that $p^k - (r+m_1M)^2$ is divided by ${p_1}^2$. Then if m_2 is another integer with the same property, then we have that $m_2 - m_1$ is divided by p_1 or r is divided by p_1. But the latter induces that p is divisible by p_1. So there are at most $\left(\left\lfloor \frac{\sqrt{(p-4)p^{k-1}}}{2p_1pM} \right\rfloor + 1\right)$ integers d which are divisible by $(p_1)^2$.

Next, we exclude d such that ${q_1}^2 \mid d$ from $S(k,p,r,a,M)$ where q_1 is not a prime divisor of M. Let m_1 be the smallest integer such that $p^k - (r+m_1M)^2$ is divided by ${q_1}^2$. Then if m_2 is another integer with the same property, then we have that $m_2 - m_1$ is divided by ${q_1}^2$ or $m_2 \equiv m_1 - \frac{2r+m_1M}{M}$ modulo ${q_1}^2$. But the latter induces that $l_2 = r + m_2M$ is congruent to $-r$ modulo M. So there are at most $\left(\left\lfloor \frac{\sqrt{(p-4)p^{k-1}}}{2{q_1}^2pM} \right\rfloor + 1\right)$ integers d which are divisible by $(q_1)^2$. Let $N(k,p,r,a,M)$ be the number of the square free integers in $S(k,p,r,a,M)$.

Then we have

$$\begin{aligned} &N(k,p,r,a,M) \\ &\quad > \Big(1 - \tfrac{1}{p_1} - \tfrac{1}{p_2} \cdots - \tfrac{1}{p_s} - \textstyle\sum_{3 \le q \le p^{k/2},(q,pM)=1} \tfrac{1}{q^2}\Big) \\ &\quad \times \tfrac{\sqrt{(p-4)p^{k-1}}}{2pM} - \big(\textstyle\sum_{3 \le q \le p^{k/2}} 1\big) + O(1) \end{aligned}$$

where $M = p_1p_2 \cdots p_s$.

By Prime number theorem and $\zeta(2) = \frac{\pi^2}{6}$,

$$\begin{aligned} &N(k,p,r,a,M) > \\ &\left(\tfrac{9}{4} - \tfrac{\pi^2}{6} + \tfrac{1}{p^2} + \textstyle\sum_{i=1}^{s}\left(\tfrac{1}{{p_i}^2} - \tfrac{1}{p_i}\right)\right)\tfrac{\sqrt{(p-4)p^{k-1}}}{2pM}. \end{aligned}$$

Since there are $p-1$ distinct nonzero residue modulo p, we showed the case when p and M are coprime.

When p divides M, we define $S(k,p,r,M) := \{p^k - l^2 \mid l : \text{even}, \ l \equiv r \mod M, \text{ and } 0 < l < \sqrt{(p-4)p^{k-1}}\}$ where r is a nonzero residue modulo M and modulo p simultaneously. Then every d in $S(k,p,r,M)$ is not divisible by p^2. Like above, we exclude d from $S(k,p,r,M)$ divisible by p_1^2 prime divisor of M or by q_1^2 not prime divisor of M. Then we can show the latter case. $\square$

For a square-free integer d, let $K = \mathbf{Q}(\sqrt{-d})$ and $h(-d)$ be the class number of K and $CL(-d)$ be the class group of K. Then we have the following lemma.

Lemma 4. *For a positive integer k and a prime number p bigger than 3, let $d = p^k - l^2$ be a* *square free integer with* $0 < l < \sqrt{(p-4)p^{k-1}}$. *Then the integer* k *divides* $h(-d)$.

Proof. Since $-d \equiv l^2 \bmod p$, a discriminant of K is a quadratic residue modulo p. So the prime p is split in K. Hence we have

$$(p) = \mathfrak{p}_1\mathfrak{p}_2$$

for the prime ideals $\mathfrak{p}_1$, $\mathfrak{p}_2$ in K.

Let m be the order of the ideal $\mathfrak{p}_1$ in a group $CL(-d)$. We assume that

$$m < k.$$

Then for the integers u and v,

$$\mathfrak{p}_1^m = \left(\frac{u+v\sqrt{-d}}{2}\right)$$

and

$$(p)^m = \left(\frac{u+v\sqrt{-d}}{2}\right)\left(\frac{u-v\sqrt{-d}}{2}\right) = \left(\frac{u^2+v^2d}{4}\right).$$

Since $\{1,-1\}$ is the set of units of an imaginary quadratic field K whose discriminant is greater than 6, we have

$$p^m = \frac{u^2+v^2d}{4}$$

This implies,

$$d > 4p^{k-1} \geq 4p^m = u^2 + v^2d.$$

So we have $v = 0$ so $\mathfrak{p}_1^m = \mathfrak{p}_2^m$, hence $\mathfrak{p}_1 = \mathfrak{p}_2$. This is a contradiction that p is split in K. Thus the order of an ideal $\mathfrak{p}_1$ in $CL(-d)$ is k. Finally, we find that k divides $h(-d)$. This complete the proof. ☐

Now, using Lemma 3 and Lemma 4, we prove Theorem 1.

Proof of Theorem 1. First, consider the case of $(p, M) = 1$. By Lemma 3 and Lemma 4, there are at least $\widetilde{c}(p,M)\sqrt{(p-4)p^{k-1}}$ imaginary quadratic fields $\mathbf{Q}(\sqrt{-d})$ with $-d \in A(r^2-p^k, M)$ and $h(-d) \equiv 0 \bmod k$.

Now, we suppose that there exist finitely many imaginary quadratic fields $\mathbf{Q}(\sqrt{-d})$ with $-d \in A(r^2-p^k, M)$ and $h(-d) \equiv 0 \bmod k$. Then there exists an integer e such that $k(\phi(M)+1)^e$ does not divide $h(-d)$ for any d we constructed. By applying Lemma 3 and Lemma 4 again, we obtain that there are at least $\widetilde{c}(p,M)\sqrt{(p-4)p^{k(\phi(M)+1)^e-1}}$ imaginary quadratic fields $\mathbf{Q}(\sqrt{-d})$ with $-d \in A(r^2-p^k, M)$ and $h(-d) \equiv 0 \bmod k$ distinct from previous ones. By repeating this process, the result we want follows.

In case that p divides M, also by Lemma 3 and Lemma 4, there are at least $\widetilde{c}(p,M)\sqrt{(p-4)p^{k-1}}$ imaginary quadratic fields $\mathbf{Q}(\sqrt{-d})$ with $-d \in A(r^2-p^k, M)$ and $h(-d) \equiv 0 \bmod k$. Since $p^{(\phi(M/p)+1)} \equiv p \bmod M$, for any positive integer e we have $p^{k(\phi(M/p)+1)^e} \equiv p^k \bmod M$. Now choose e such that $k(\phi(M/p)+1)^e$ does not divide $h(-d)$ for any d we constructed. Then, we can also show this case similarly like above.

When M is a prime number, using Perron's Theorem [5] of distribution of quadratic residues of $\mathbf{Z}/q\mathbf{Z}$, we can get the following result.

Corollary 5. *If* $q = 4s-1$ (*resp.* $q = 4s+1$) *is a prime number bigger than* 3, *then there are at least* $3s$ (*resp.* $3s+1$) *distinct arithmetic progressions modulo* q *satisfying Theorem* 1. *In particular, if* $q = 5$, *then, for any fixed* k, *there are infinitely many positive square-free* d *such that*

$$h(-d) \equiv 0 \bmod k \text{ and } -d \in A(a, 5)$$

where a *is any fixed integer* $\in \{0,1,3,4\}$.

Proof. In Theorem 1, choose $M = q$ and $p = q$ where q is a prime number bigger than 3. Then, if $q = 4s-1$, there are $2s-1$ non-zero quadratic residues modulo q. Therefore, there exist $2s-1$ arithmetic progressions modulo q satisfying Theorem 1. If we put $p = q'$ which is congruent 1 modulo q, then, by Perron's Theorem on the distribution of quadratic residues of $\mathbf{Z}/q\mathbf{Z}$, we have additional $s+1$ arithmetic progressions modulo q holding Theorem 1. In case of $q = 4s+1$, we can show that there are $3s+1$ arithmetic progressions modulo q satisfying Theorem 1 with the same argument. ☐

Remark 2. We can extend Theorem 1 for an odd integer $M = p_1^{e_1}p_2^{e_2}\cdots p_s^{e_s}$ or $M = pp_1^{e_1}p_2^{e_2}\cdots p_s^{e_s}$. Then we have more restriction on a quadratic residue m modulo M. The restriction is that $p^k - m$ is not congruent to 0 modulo p_i^2 for all $e_i \geq 2$.

3. Proof of Theorem 2. For convenience, we state Theorem 2 here again.

Theorem 2. *Let* $r(n)$ *be the representation numbers of integers as sum of three squares. Then,*
1) *For any given integer* k, *there are infinitely many square-free* n *such that*

$$n \equiv 1 \bmod 4 \text{ and } r(n) \equiv 0 \bmod 12k.$$

2) *For any given odd integer* k, *there are infinitely many square-free* n *such that*

$$n \equiv 2 \mod 4 \text{ and } r(n) \equiv 0 \mod 12k.$$

3) *For any given odd integer k, there are infinitely many square-free n such that*

$$n \equiv 3 \mod 8 \text{ and } r(n) \equiv 0 \mod 24k.$$

Proof. From the relationship between $r(n)$ and the class number of $\mathbf{Q}(\sqrt{-n})$ mentioned in the Introduction, we can see easily the following identity. For a positive square-free integer n bigger than 3,

$$r(n) = \begin{cases} 12h(-n) & \text{if } \; n \equiv 1,2 \mod 4 \\ 24h(-n) & \text{if } \; n \equiv 3 \mod 8. \end{cases}$$

Hence, Ankeny and Chowla [1] implies the first statement as we explained in the Introduction.

Secondly, for an odd integer k, we consider square-free integers n of the form $n = 7^k - l^2$ where l is of the form $1 + 4m \times 7$. Such n is congruent to 2 modulo 4 and $h(-n)$ is divisible by k by Lemma 4. Since n is always congruent to 2 modulo 4, n is not divisibly by 4. Then by the argument of the proof of Lemma 3, we can show that there are infinitely many such n. This together with the above identity proves the second statement.

Thirdly, for an odd integer k, we consider square-free integer n of the form $n = 7^k - l^2$ where l is of the form $2 + 4m \times 7$. Then we have $n \equiv 3$ modulo 8 and $h(-n)$ is divisible by k by Lemma 4. Then by the argument of the proof of Lemma 3, we can show that there are infinitely many such n. This together with the above identity proves the third statement. $\square$

Remark 3. Using Lemma 4, we can find n satisfying Theorem 2 explicitly. For example, if we put $p = 5$, $k = 6$, then $r(n)$ is divisible by 72 and $n \equiv 1 \mod 4$ for all $n \in \{12709, 12921, 13321, 13861, 14181, 14329, 14469, 14601, 15049, 15301, 15369, 15429, 15481, 15589, 15621\}$.

Acknowledgements. We would like thank Prof. Dongho Byeon in Seoul National University who suggested the problem as a topic of Master thesis and advised to use the idea of Ankeny and Chowla [1].

References

[1] N. C. Ankeny and S. Chowla, On the divisibility of the class number of quadratic fields, Pacific J. Math. **5** (1955), 321–324.

[2] W. Kohnen and K. Ono, Indivisibility of class numbers of imaginary quadratic fields and orders of Tate-Shafarevich groups of elliptic curves with complex multiplication, Invent. Math. **135** (1999), no. 2, 387–398.

[3] S.-N. Kuroda, On the class number of imaginary quadratic number fields, Proc. Japan Acad. **40** (1964), 365–367.

[4] T. Nagel, Über die Klassenzahl imäginar-quadratischer Zahkörper, Abh. Math. Seminar Univ. Hamburg **1** (1922) 140–150.

[5] O. Perron, Bemerkungen über die Verteilung der quadratischen Reste, Math. Z. **56** (1952), 122–130.

[6] K. Soundararajan, Divisibility of class numbers of imaginary quadratic fields, J. London Math. Soc. (2) **61** (2000), no. 3, 681–690.