Tôhoku Math. Journ.
22(1970), 604-612.

ON THE LENGTHS AND THE NUMBERS OF CONGRUENCE CLASSES OF CLOSED GEODESICS IN GRASSMANN MANIFOLDS

YUNG-CHOW WONG AND SAMUEL S. H. YOUNG

(Received January 19, 1970)

1. Introduction. Let F be the field of real numbers, the field of complex numbers, or the field of real quaternions; F^{n+m} a left $(n+m)$-dimensional Hermitian vector space over F; and $G_n(F^{n+m})$ the Grassmann manifold of n-planes in F^{n+m} provided with the Riemannian metric with respect to which the distance between two points A and B in $G_n(F^{n+m})$ is equal to the square root of the sum of the squares of the angles between the n-planes A and B in F^{n+m}. This Riemannian metric is invariant under the group of transformations induced from the group of motions in F^{n+m}. A maximal set of curves in $G_n(F^{n+m})$ invariant under this group of transformations in $G_n(F^{n+m})$ is called a congruence class of curves in $G_n(F^{n+m})$.

Recently, a method of studying the differential geometry of $G_n(F^{n+m})$ through a study of the geometry of n-planes in F^{n+m} was initiated by one of us (see Wong [5], [6] and [7]). Among the results announced in [5] are the following ones concerning closed geodesics:

THEOREM 1.1. (a) *There is a one-one correspondence between the set of congruence classes of closed geodesics in* $G_n(F^{n+m})$ *and the set of ratios* $n_1 : n_2 : \cdots : n_r$, *where* $r=\min(n, m)$ *and the* n_i*'s are non-negative integers, arranged in descending order and not all zero.*

(b) *The closed geodesics* $G_n(F^{n+m})$ *corresponding to the ratios* $n_1 : n_2 : \cdots : n_r$ *are of length* $(m_1^2+m_2^2+\cdots+m_r^2)^{1/2}\pi$, *where the* m_i*'s are non-negative integers proportional to the* n_i*'s and having no common factor other than* 1.

When one studies the geodesics in a particular Riemannian manifold in which closed geodesics exist, it is natural to ask:

(1) What are the lengths L of its closed geodesics?
(2) For a given L, what is the number of congruence classes of closed geodesics of the same length L? Or equivalently,
(2′) What are the lengths of those closed geodesics for which there are exactly $k(=1, 2, \cdots)$ congruence classes?

The results in Theorem 1.1 show that for a $G_n(F^{n+m})$ these questions become respectively the following ones in number theory:

(1*) What are those integers L that can be represented as the sum of $r=\min(n, m)(\geqq 1)$ perfect squares having no common factor other than 1?

(2*) For a given L, what is the number of such representations? Or equivalently,

(2'*) What are those integers that have exactly $k(=1, 2, \cdots)$ such representations?

Questions (1*) and (2*) (or (2*)) become trivial if $r=1$. For $r\geqq 2$, these questions seem to have been completely answered only for $r=2$ though there exists an extensive literature on "sums of squares" (see [1]). In this paper, using some known results in number theory, we obtain a complete answer to question (1), an answer to question (2) for the case $\min(n, m)=1$ or 2, and an answer to question (2) for the case $k=1$. Although it is likely that, for other small values of k, an answer to (2') for the case $\min(n, m)\geqq 3$ can be obtained by using a similar method, we are content to leave it to those who are more expert in number theory.

In §§2-6, we state and prove our results. For convenience of the reader, we collect in §7 some known results in number thory that we have to use.

2. The case $\min(n, m)=1$ or 2. For these two cases, we have a complete answer to questions (1) and (2).

THEOREM 2.1. *In a $G_n(F^{n+m})$, where $\min(n, m)=1$, all the geodesics are closed and are of length π. Moreover, there is exactly one congruences class.*

PROOF. This is trivial and also well known. (See [5], Corollary to Theorem 11).

THEOREM 2.2. *In a $G_n(F^{n+m})$, where $\min(n, m)=2$,*

(a) *a closed geodesic can and can only be of length*

$$\pi,\ \sqrt{2}\pi,\quad \text{or}\quad (2^{\nu}p_1^{\alpha_1}\cdots p_{\mu}^{\alpha_{\mu}})^{1/2}\pi,$$

where $\nu=0$ or 1; $\mu\geqq 1$; the p_i's are distinct primes $\equiv 1 \pmod 4$; and the α_i's are positive integers.

(b) *There are one and only one congruence class of closed geodesics of length π, one and only one of length $\sqrt{2}\pi$, and exactly $2^{\mu-1}$ of length $(2^{\nu}p_1^{\alpha_1}\cdots p_{\mu}^{\alpha_{\mu}})^{1/2}\pi$.*

PROOF. This is a direct consequence of some known results in number theory (see §7, Theorems A and B).

THEOREM 2.3. *Let* (p_i) *be the increasing sequence of primes* $\equiv 1 \pmod 4$. *Then in any* $G_n(F^{n+m})$, *where* $\min(n, m)=2$, *the following is true: Among the closed geodesics of the same length of which there are exactly* $2^{\mu-1}(\mu>1)$ *congruence classes, the shortest ones are of length* $L_\mu=(p_1p_2\cdots p_\mu)^{1/2}\pi$. *In particular, among the closed geodesics of the same length of which there are exactly two, four or eight congruence classes, the shortest ones are of lengths* $\sqrt{65}\pi$, $\sqrt{1105}\pi$ *or* $\sqrt{32045}\pi$, *respectively.*

PROOF. This follows from Theorem 2.2 and the fact that $(p_i)=(5, 13, 17, 29, \cdots)$.

3. The case $\min(n, m)\geqq 3$. A complete answer to question (1) is given in Theorem 3.1 below, where, for completeness, part (a) of Theorem 2.2 is included.

THEOREM 3.1. *In a* $G_n(F^{n+m})$, *where* $\min(n, m)=r\geqq 2$, *there are closed geodesics of length* $\sqrt{L}\pi$ *for every positive integer* L *except in the following cases:*

(a) $r=2$ *and* L *contains a prime factor* $\equiv 3 \pmod 4$.
(b) $r=3$ *and* $L\equiv 0, 4$ *or* $7 \pmod 8$.
(c) $r=4$ *and* $L\equiv 0 \pmod 8$.

The next two theorems give an answer to question (2′) for the case $k=1$.

THEOREM 3.2. *In a* $G_n(F^{n+m})$, *where* $\min(n, m)=r\geqq 4$, *the only cases in which there is exactly one congruence class of closed geodesics of length* $\sqrt{L}\pi$ *are the following:*

(a) $r\geqq 8$: $L=1, 2, 3,$ *or* 4.
(b) $r=7$; $L=1, 2, 3, 4$ *or* 8.
(c) $r=6$; $L=1, 2, 3, 4, 7, 8$ *or* 16.
(d) $r=5$; $L=1, 2, 3, 4, 6, 7, 8, 9, 12, 15, 16$ *or* 24.
(e) $r=4$; $L=1, 2, 3, 4, 5, 6, 7, 9, 11, 12, 14, 15, 20, 23, 36$ *or* 44.

THEOREM 3.3. *Let* L *be a given positive integer and* h *the number of classes in the principal genus of the properly primitive binary quadratic forms of determinant* $-L$. *Then in a* $G_n(F^{n+m})$, *where* $\min(n, m)=3$, *there is exactly one congruence class of closed geodesics of length* $\sqrt{L}\pi$ *iff* L *has one of the*

following forms:

(a) $L=p^{\alpha}$, *where* p *is an odd prime and* $\alpha\geqq 1$.
  (i) $p\equiv 3 \pmod 8$; α *is even and* $h=1$, *or* α *is odd and* $h=3$.
  (ii) $p\equiv 5 \pmod 8$; $h=1$.
  (iii) $p\equiv 7 \pmod 8$; α *is even and* $h=2$.

(b) $L=2p^{\beta}$, *where* p *is an odd prime and* $\beta\geqq 1$.
  (i) $p\equiv 3$ *or* $5 \pmod 8$; $h=1$.
  (ii) $p\equiv 7 \pmod 8$; $h=2$.

(c) $L=p_1^{\alpha}p_2^{\beta}$, *where* p_1, p_2 *are distinct odd primes and* $\alpha\geqq 1$, $\beta\geqq 1$.
  (i) $p_1\equiv 1 \pmod 4$, $p_2\equiv 7 \pmod 8$; β *is even and* $h=1$.
  (ii) $p_1\equiv 3$ *or* $7 \pmod 8$, $p_2\equiv 7 \pmod 8$; α, β *are either both odd or both even and* $h=1$.
  (iii) $p_1\equiv 3 \pmod 8$, $p_2\equiv 5 \pmod 8$; α *is even and* $h=1$.
  (iv) $p_1\equiv 3 \pmod 8$, $p_2\equiv 5$ *or* $7 \pmod 8$; α *is odd,* β *is even and* $h=3$.
  (v) $p_1\equiv 5 \pmod 8$, $p_2\equiv 7 \pmod 8$; α, β *are both odd and* $h=3$.

(d) $L=2p_1^{\alpha}p_2^{\beta}$, *where* p_1, p_2 *are distinct odd primes and* $\alpha\geqq 1$, $\beta\geqq 1$.
  (i) $p_1\equiv 3 \pmod 8$, $p_2\equiv 5 \pmod 8$; $h=1$.
  (ii) $p_1\equiv 7 \pmod 8$; $h=1$.

In particular, the values of L *not exceeding* 100 *are as follows*: 1, 2, 3, 5, 6, 9, 10, 11, 13, 14, 18, 19, 21, 22, 25, 27, 30, 35, 37, 42, 43, 45, 46, 49, 58, 67, 70, 75, 78, 91 *and* 93.

4. Proof of Theorem 3.1. The theorem is a direct consequence of the following proposition which furnishes a complete answer to question (1*) stated in §2. We shall use the symbol $\boxed{r}$ to denote a sum of r perfect squares and $\boxed{\underline{r}}$ to denote an $\boxed{r}$ whose summands do not have any common factor other than 1. According to this definition, a positive number L can be expressed as $\boxed{r}'$ with only one non-zero summand iff $L=1$. Therefore, we can assume hereafter that in the representation of L as $\boxed{r}'$, at least two of the summands are non-zero so that $L>1$.

PROPOSITION 4.1. *Let* L *be a given integer* >1. *Then*
(a) L *can be expressed as* $\boxed{2}'$ *iff* L *does not contain any prime factor* $\equiv 3 \pmod 4$.
(b) L *can be expressed as* $\boxed{3}'$ *iff* $L\equiv 1, 2, 3, 5$ *or* $6 \pmod 8$.
(c) L *can be expressed as* $\boxed{4}$ *iff* $L\not\equiv 0 \pmod 8$.
(d) L *can always be expressed as* $\boxed{r}$ *if* $r\geqq 5$.

PROOF. (a) is well-known (see §7, Theorem A). An elegant proof of (b) was given by Dirichlet using the theory of ternary quadratic forms ([1], pp. 263-264).

(c) is an easy consequence of (b). To prove (d), we assume that $L=1+u$, where u is a positive integer. Since every positive integer can be expressed as $\boxed{4}$ (see §7, Theorem D), L can be represented as $\boxed{5}'$, and hence also as $\boxed{r}'$ with $r>5$, by adding a suitable number of 0^2.

5. Proof of Theorem 3.2. For $r\geqq 3$, question (2*) in number theory as mentioned in §1 has only been partially auswered ([1], [3], [4]). Let us denote by $R(L,r)$ the number of representations of L as $\boxed{r}$ if representations differing in arrangement of the squares and signs of their roots are counted as distinct, and by $P(L,r)$ if difference in arrangements and signs is disregarded. As far as the authors are aware, whereas formulas for $R(L,r)$ for $r=3,4$, and probably for certain other values of r also, have been obtained, the corresponding formulas for $P(L,r)$ are still not known. Therefore, we shall confine ourselves to the case $k=1$ of question (2'*), i.e., we shall give an answer to the question:

(3*) For a fixed $r\geqq 3$, what are those integers L that be represented uniquely as $\boxed{r}'$?

If $r\geqq 4$, the possible values of L for which we are seeking are finite in number. In fact, we have

PROPOSITION 5.1. *Let r and L be two positive integers and $r\geqq 4$. Then the only cases in which L can be represented uniquely as $\boxed{r}'$ are those given in Theorem 3.2.*

PROOF. We have to consider the two cases, $r\geqq 5$ and $r=4$ separately.

To prove the assertion for the case $r\geqq 5$, we first find some small number c such that every integer $>c$ has at least two distinct representations as $\boxed{r}'$. If c is small enough, the values of L can then be found by direct verification or other appropriate methods. As an illustration, we give a detailed proof for the case $r=6$.

Let $L=25+u$, where u is a positive integer. Then we can always choose integers s_1, s_2, s_3 and s_4 so that the following are two distinct representations of L as $\boxed{6}'$:

$$s_1^2+s_2^2+s_3^2+s_4^2+4^2+3^2,$$

$$s_1^2+s_2^2+s_3^2+s_4^2+5^2+0^2.$$

In fact, this is possible if $u\not\equiv 0 \pmod 8$, by Proposition 4.1(c). If $u\equiv 0 \pmod 8$, let us write $u=2^{2b}(2^v w)$, where w is an odd integer, $v=0$ or 1, and $2b+v\equiv 0 \pmod 3$. Then $2^v w\not\equiv 0 \pmod 8$, and therefore it can be expressed as $t_1^2+t_2^2+t_3^2+t_4^2$, where the t_i's have no common factor other than 1. Let $s_i=2^b t_i$, and we obtain the required representations. Hence, all values of L exceeding 25 need not be considered.

It can be easily verified that if $L\leqq 9$, the only numbers that admit unique

representation as [6]′ are 1, 2, 3, 4, 7 and 8. If $L=9+v, 1\leqq v\leqq 16$, then we can choose integers q_1, q_2 and q_3 so that the following two representations of L as [6]′ are distinct

$$q_1^2+q_2^2+q_3^2+2^2+2^2+1^2,$$

$$q_1^2+q_2^2+q_3^2+3^2+0^2+0^2$$

unless $v=4^a(8b+7)$(cf. §7, Theorem C), i. e., unless $v=7$ or 15. If $v=7$, we have $L=16$ which has indeed unique representation as [6]′. If $v=15$, we have $L=24$ which however has two distinct representations as [6].

This completes the proof of our assertion for the case $r=6$. Our assertions for the other values of $r\geqq 5$ can be proved in a similar manner.

We now consider the case $r=4$. Let us write $L=2^au$, where u is a positive odd integer and $a\geqq 0$. By Proposition 4.1(c), if $a\geqq 3$, then $L=2^au$ cannot be represented as [4]′. Therefore, we need consider only those L which are of the form u, $2u$, or $4u$. For these, we have [4, p. 249]:

$$(5.1)_1 \qquad R(u,4)=8u\{S(v)v^{-1}\},$$

$$(5.1)_2 \qquad R(2u,4)=24u\{S(v)v^{-1}\},$$

$$(5.1)_3 \qquad R(4u,4)=16u\{S(v)v^{-1}\},$$

where v is the largest square-free divisor of u and $S(v)$ is the sum of divisors of v.

Also, it is obvious that $L=1$, 2, 3, or 4 has a unique representation as [4]′. Therefore, we may assume that $L>4$.

Now let $L>4$. Then every representation of L as [4]′ must have one of the following forms:

(5.2)

(A) $x^2+y^2+0^2+0^2$,
(B) $x^2+x^2+x^2+y^2$,
(C) $x^2+x^2+y^2+0^2$,
(D) $x^2+x^2+y^2+y^2$,
(E) $x^2+y^2+z^2+0^2$,
(F) $x^2+x^2+y^2+z^2$,
(G) $x^2+y^2+z^2+w^2$,

where x, y, z and w denote distinct integers. By computing the number of arrangements of the squares and the signs of their roots, we find that, to each representation of L as [4]′ in the form (5.2)(A), (B), (C), (D), (E), (F) or (G) counted in $P(L,4)$, there correspond, respectively, 48, 64, 96, 96, 192, 192, or 384 representations counted in $R(L,4)$. Hence,

(5.3) $$P(L, 4) = R(L, 4)/k \text{ for some } k \leqq 384.$$

We shall now consider separately the cases where L is of the form u, $2u$ or $4u$.

Case (i). Let $L=u=p^{\alpha}$, where p is an odd prime and α a positive integer. Then by $(5.1)_1$ and (5.3), we have $P(L, 4) = p^{\alpha-1}(p+1)/k_1$ with $k_1 \leqq 48$ (see §7, Theorem F). In order that $P(L, 4)=1$, it is necessary that $\alpha<3$ and $k_1=6, 8, 12, 24$ or 48. By simple computation, we see that the possible values of L are 47, 23, 11, 9, 7 or 5, and from these 47 has to be discarded since it has two distinct representations as [4]'.

Now let $L=u=p_1^{\alpha}p_2^{\beta}$, where p_1, p_2 are distinct odd primes and α, β positive integers. It can be shown that $P(L, 4) = 1$ iff $\alpha = \beta = 1$ and $(p_1, p_2) = (3, 5)$. The corresponding value of L is 15. If L has more than two distinct odd prime factors, then the condition $P(L, 4) = 1$ cannot be satisfied.

Case (ii). Let $L = 2u = 2p^{\alpha}$, where p is an odd prime and α a positive integer. If L has a unique representation as [4]', then it can only be represented in exactly one of the forms given in (5.2). By $(5.1)_2$ and (5.3), a necessary condition for this is that $24p^{\alpha-1}(p+1)$ is divisible by 48, 64, 96, 192 or 384. Furthermore, if $\alpha>1$, then $P(L, 4)>1$. From this we deduce that $P(L, 4)=1$ iff $p=7$ or 3, corresponding to which we obtain $L=14$ or 6. If u has two or more distinct odd prime factors, then L cannot be uniquely represented as [4]'.

Case (iii). Let $L=4u=4p^{\alpha}$, where p is an odd prime and α a positive integer. Using $(5.1)_3$ and (5.3) and proceeding as in the previous two cases, we obtain $L=44$, 20 or 12 if $\alpha=1$, and $L = 36$ if $\alpha = 2$. For all other values of $L = 4u$, it can be easily shown that unique representation of L as [4]' is impossible.

Proposition 5.1 is thus completely proved from which Theorem 3.2 follows.

6. Proof of Theorem 3.3. For the case $r = 3$, question (3*) stated in the first paragraph of §5 can be answered by using the theory of binary quadratic forms (see [2]). In fact, we have

PROPOSITION 6.1. *Let L be a given positive integer and h the number of classes in the principal genus of the properly primitive binary quadratic forms of determinant $-L$. Then L can be represented uniquely as [3]' iff it has one of the forms as given in Theorem* 3.3.

PROOF. By a theorem due to Gauss ([1], p. 262), we have

$$(6.1)_1 \qquad R(L,3) = 3\cdot 2^{\mu+2}h \text{ if } L \equiv 1, 2, 5 \text{ or } 6 \pmod 8,$$

$$(6.1)_2 \qquad R(L,3) = 2^{\mu+2}h \text{ if } L \equiv 3 \pmod 8,$$

where μ denotes the number of distinct odd prime factors of L.

Now every representation of $L(>3)$ as [3]′ must have one of the following forms:

$$(6.2) \qquad \begin{array}{ll} \text{(A)} & x^2+y^2+0^2, \\ \text{(B)} & x^2+x^2+y^2, \\ \text{(C)} & x^2+y^2+z^2, \end{array}$$

where x, y, z are distinct integers. It is easy to see that if L is uniquely representable as [3] in the form (6.2)(C), then $R(L,3)=48$. On the other hand, if L is uniquely representable as [3]′ in the form (6.2)(A) or (B), then $R(L,3)=24$. Furthermore, $\mu<3$ is a necessary condition for $P(L,3)=1$.

Using the above observations and some known results in number theory (see §7, Theorems A and E), we can obtain from $(6.1)_1$ and $(6.1)_2$ all the desired values of L as given in Theorem 3.3.

Proposition 6.1 is thus proved and Theorem 3.3 is just a restatement of the results in geometric language.

7. Some Known Results in Number Theory. Fos convenience of the reader, we collect here some known results in number theory that we have used.

THEOREM A. *A positive integer L can be expressed as a sum of two relatively prime perfect squares iff it is of the form $2^{\nu}p_1^{\alpha_1}\cdots p_\mu^{\alpha_\mu}$, where $\nu=0$ or 1; $\mu\geqq 1$; the p_i's are distinct primes $\equiv 1 \pmod 4$, and the α_i's are positive integers* [3, pp. 297-299, Theorems 366, 367 and 368].

THEOREM B. *When L has μ distinct prime factors each $\equiv 1 \pmod 4$, there are exactly $2^{\mu-1}$ ways of expressing L as a sum of two relatively prime perfect squares, if difference in arrangement of the squares and signs of their roots is disregarded* [2, p. 76, Theorem 62].

THEOREM C. *A positive integer L can be expressed as a sum of three perfect squares iff L is not of the form $4^a(8b+7)$, where $a\geqq 0$, $b\geqq 0$* [4, pp.161-162, Theorems 186 and 187].

THEOREM D. *Every positive integer can be expressed as a sum of four perfect squares* [3, p. 300, Theorem 369].

THEOREM E. *A positive integer L can be expressed as a sum of a perfect square and the double of a perfect square iff all of its odd prime factors are* $\equiv 1$ *or* $3 \pmod 8$ [2, p. 76, Ex. XX2].

THEOREM F. *Let* $L = \prod_{i=1}^{k} p_i^{\alpha_i}$, *where the* p_i*'s are distinct primes and the* α_i*'s are positive integers. Then the sum of divisors* $S(L)$ *of* L *is given by*

$$S(L) = \prod_{i=1}^{k} \left(\frac{p_i^{\alpha_i+1} - 1}{p_i - 1} \right)$$

[4, p. 29, Theorem 31].

REFERENCES

[1] L. E. DICKSON, History of the Theory of Numbers, vol. II, reprinted, Chelsea, 1952.
[2] L. E. DICKSON, Introduction to the Theory of Numbers, New Dover Edition, 1957.
[3] G. H. HARDY AND E. M. WRIGHT, An Introduction to the Theory of Numbers, Second Edition, Oxford University Press, 1945.
[4] E. LANDAU, Elementary Number Theory (English translation by J. E. Goodman), Chelsea, 1958.
[5] Y. C. WONG, Differential geometry of Grassmann manifolds, Proc. Nat. Acad. Sci., U. S. A., 57(1967), 589-594.
[6] Y. C. WONG, Conjugate loci in Grassmann manifolds, Bull. Amer. Math. Soc., 74(1968), 240-245.
[7] Y. C. WONG, Sectional curvature of Grassmann manifolds, Proc. Nat. Acad. Sci. U. S. A., 60(1969), 75-79.

DEPARTMENT OF MATHEMATICS
UNIVERSITY OF HONG KONG
HONG KONG