REFERENCES

1. Adams,W.W. and Goldstein,L.J., Introduction to Number Theory, New Jersey, Prentice-Hall,1976.

2. Stewort,I.N. and Tall,D.O., Algebraic Number Theory, New York, Johnwiley&Sons,1979.

3. Fraleigh,J.B., A First Course in Abstract Algebra, Massachusetts, Addison-Wesley Publishing Co, 1976.

APPENDIX I

We shall review concept in [2] to verify that in any quadratic fields, the concepts of the fractional ideals and that spg-modules are the same.

An <u>ideal</u> is a nonemty subset I of a ring R such that if $r,s \in I$, then $r-s \in I$; and if $r \in R$, $s \in I$ then $rs \in I$. The <u>fraction ideals</u> of I_d are subsets of $\mathbb{Q}(\sqrt{d})$ of the form $c^{-1}I$, where I is an ideal of I_d and c is a nonzero element of I_d.

<u>Theorem A.</u> Let $M \subseteq \mathbb{Q}(\sqrt{d})$ and $M \neq \{0\}$. Then M is an integral module if and only if M is an ideal of I_d.

<u>Proof.</u> Let $M \subseteq \mathbb{Q}(\sqrt{d})$ and $M \neq \{0\}$.
First, we assume that M is an integral module. So $M \subseteq I_d$. It is clear that if $r,s \in M$, then $r-s \in M$. Let $x \in M$ and $a \in I_d$. Then $ax \in I_d M = M$. Hence, M is an ideal of I_d.
To prove the converse, we assume that M is an ideal of I_d. It is clear that, $M \subseteq I_d$, $MI_d = M$ and M is a $\mathbb{Z}$-module. Let r be any nonzero element in M. So $\{r, r\omega_d\}$ is a basis of $\mathbb{Q}(\sqrt{d})$ and is contained in M. Therefore, M is an integral module. #

<u>Theorem B.</u> Let $M \subseteq \mathbb{Q}(\sqrt{d})$ and $M \neq \{0\}$. Then M is an spg-module if and only if M is a fractional ideal of I_d.

<u>Proof.</u> Let $M \subseteq \mathbb{Q}(\sqrt{d})$ and $M \neq \{0\}$.
First, we assume that M is an spg-module. Then there

exists a positive rational integer k such that $kM \subseteq I_d$. So kM is an integral module. By Theorem A, kM is an ideal of I_d. Since $k \in I_d$, we conclude that $M = k^{-1}(kM)$ is a fractional ideal of I_d.

To prove the converse, we assume that M is a fractional ideal of I_d. Then $M = c^{-1}B$, where B is an ideal of I_d and c isanonzero element in I_d. By Theorem A, B is an integral module. So B is an spg-module. Since $c^{-1}I_d$ is an spg-module, then $M = (c^{-1}I_d)B = c^{-1}B$ is an spg-module.

#

APPENDIX II

We shall review the concepts of congruences and some results on quadratic congruences.

Definition 1. Let n be a positive rational integer and x,y be rational integers. We say that x and y are congruent modulo n , written $x \equiv y \pmod{n}$, provided that x-y is divisible by n. If x is not congruent to y modulo n, we write $x \not\equiv y \pmod{n}$.

Theorem 2. ([1] , proposition 3.2.1.) Let a,b,c be rational integers. Then the followings hold:

(i). $a \equiv a \pmod{n}$.

(ii). If $a \equiv b \pmod{n}$, then $b \equiv a \pmod{n}$.

(iii). if $a \equiv b \pmod{n}$, and $b \equiv c \pmod{n}$, then $a \equiv c \pmod{n}$.

Remark 3. Let $f(x) \equiv 0 \pmod{n}$ be a polynomial congruence We see that x is a solution to the congruence, then any y such that $x \equiv y \pmod{n}$ is also a solution.

Definition 4. Let x and y be any two solutionsof $f(x) \equiv 0 \pmod{n}$. We say that x and y are different if $x \not\equiv y \pmod{n}$.

Theorem 5. ([1] , Theorem 3.4.1.) Let $n = p_1^{a_1} p_2^{a_2} \ldots p_t^{a_t}$ be any positive rational integer, where $p_1, \ldots p_t$ are distinct rational primes. A rational integer x is a solution of the congruence $f(x) \equiv 0 \pmod{n}$ if and only if x satisfies a system of congruences

$$x \equiv b_1 \pmod{p_1^{a_1}},$$
$$\vdots$$
$$x \equiv b_t \pmod{p_t^{a_t}},$$

where b is a solution of the congruence

$$f(x) \equiv 0 \pmod{p_i^{a_i}}. \quad (i = 1,2,\ldots,t)$$

Theorem 6. ([1], Theorem 3.4.2.(Chinese Remainder Theorem)). Suppose that the rational positive integers $m_1,\ldots,m_t$ are ralatively prime in pairs. Let $b_1,..,b_t$ be arbitrary rational integers. Then the congruences

$$x \equiv b_1 \pmod{m_1},$$
$$\vdots$$
$$x \equiv b_t \pmod{m_t}$$

have a solution. Moreover, the solution is unique modulo $m_1 \ldots . m_t$.

Definition 7. Let p be a rational prime and a be any rational integer such that $p \nmid a$. We say that a is quadratic residue modulo p provided that $x^2 \equiv a \pmod{p}$ has a solution. Otherwise, we say that a is a quadratic nonresidue modulo p.

Theorem 8 ([1], Lemma 4.2.3.) Suppose that p is an odd rational prime and a is a quadratic residue modulo p, $p \nmid a$. Then the congruence $x^2 \equiv a \pmod{p}$ has exactly two distinct solutions.

Theorem 9. ([1], Proposition 4.2.4.) Let p be an odd rational prime and a be any rational integer such that $p \nmid a$. Then a is a quadratic residue modulo p if and only if a is

congruenct to one of $1^2, 2^2, \ldots, (\frac{p-1}{2})^2$ modulo p.

Example 10. We shall verify that $x^2 \equiv -31 \pmod{12}$ has no solution. By Theorem 5 and Theorem 6, we know that $x^2 \equiv -31 \pmod{12}$ is solvable if and only if $x^2 \equiv -31 \pmod{4}$ and $x^2 \equiv -31 \pmod{3}$ are solvable. By Theorem 9, we can verify that $x^2 \equiv 2 \pmod{3}$ is not solvable. Since $-31 \equiv 2 \pmod{3}$, we conclude that $x^2 \equiv -31 \pmod{3}$ is not solvable. Therefore, $x^2 \equiv -31 \pmod{12}$ is not solvable. #

Example 11. We shall find all solutions of $x^2 \equiv -24 \pmod{20}$. By Theorem 5 and Theorem 6, we can conclude that $x^2 \equiv -24 \pmod{20}$ is solvable if and only if $x^2 \equiv -24 \pmod{5}$ and $x^2 \equiv -24 \pmod{4}$ are solvable. By Theorem 8, if $x^2 \equiv -24 \pmod{5}$ is solvable, then it has exactly two distinct solutions. Therefore, $x^2 \equiv -24 \pmod{20}$ has at most two distinct solutions. Using Theorem 9, we can verify that ± 4 are distinct solutions of $x^2 \equiv -24 \pmod{5}$. It is clear that ± 4 are also solutions of $x^2 \equiv -24 \pmod{4}$. By Theorem 5, we can conclude that ± 4 are solutions of $x^2 \equiv -24 \pmod{20}$. Therefore, the set $\{\pm 4 + 20n \mid n \in \mathbb{Z}\}$ is the set of all solutions of $x^2 \equiv -24 \pmod{20}$.

#

VITA

Name : Mr. Somchit Chotchaisthit

Degree : B.Sc.(Education), 1979.
Chiengmai University.

Scholarship : University Development Commission (U.D.C),
Thai Government.