Internat. J. Math. & Math. Sci.
Vol. 1 (1978) 75-86

COMPLETE RESIDUE SYSTEMS IN THE QUADRATIC DOMAIN $Z(e^{2\pi i/3})$

GERALD E. BERGUM
Department of Mathematics
South Dakota State University
Brookings, South Dakota 57006

(Received April 30, 1976)

ABSTRACT. Several representations for a complete residue system in the Euclidean domain $Z(\omega)$ are presented in this paper.

1. INTRODUCTION.

Throughout this paper, small case Latin letters with the exception of e and i will represent rational integers. The Latin letters e and i respectively represent the base for the natural logarithms and the imaginary unit. We let $\omega = e^{2\pi i/3}$ and $Z(\omega) = \{a + b\omega | a,b \in Z\}$. The Greek letters α, β, γ, δ, σ, and μ will always represent integers in $Z(\omega)$.

We will illustrate the integers in $Z(\omega)$ by the lattice points in a Cartesian coordinate system formed by the intersections of the lines through the points $(x,0)$, x a real integer, and making angles of 60° or 120° with the x-axis. This system is composed of equilateral-triangles.

In Uspensky and Heaslet (4), we find many representations for a complete residue system modulo n. Two of the most well-known complete residue systems molulo n are the set of integers $\{0, 1, 2, \cdots, n-1\}$ and the set of integers $\{x \mid -n/2 < x \leq n/2\}$. The latter representation is the one with least absolute values.

Jordan and Portratz (2) exhibit several representations for a complete residue system in the Gaussian integers and in Potratz (3) we find several representations for a complete residue system in the quadratic Euclidean domain $Z(\sqrt{-2}) = \{a + b\sqrt{-2} \mid a,b \in Z\}$. It is the purpose of this paper to exhibit several representations for a complete residue system in the Euclidean domain $Z(\omega)$.

We say that $\alpha \mid \beta$ iff there exists a δ such that $\beta = \alpha\delta$. Furthermore, $\alpha \equiv \beta (\text{mod } \gamma)$ iff $\gamma \mid (\alpha - \beta)$. It is a trivial matter to show that congruence modulo γ is an equivalence relation on $Z(\omega)$ and hence, as in the real case, it is reasonable to define a complete residue system modulo γ as a nonempty collection S of elements in $Z(\omega)$ such that (1) no two elements of S are congruent modulo γ, and (2) every element of $Z(\omega)$ not in S is congruent to some element in S. A complete residue system modulo γ is abbreviated as C.R.S. (mod γ). We define the norm of γ, denoted by $N(\gamma)$, as $N(\gamma) = |\gamma|^2$. If $\gamma = a + b\omega$ then $N(\gamma) = a^2 - ab + b^2$.

2. REPRESENTATION I. The first representation of a C.R.S. (mod γ) appears to be a natural generalization of $\{0, 1, 2, \cdots, n-1\}$ modulo n. Let $\gamma = a + b\omega$, $d = (a, b)$, and $\gamma = d(a_1 + b_1\omega) = d\mu$.

THEOREM 2.1. If d is even, $T_1 = \{x + y\sqrt{3}i \mid 0 \leq x \leq d|\mu|^2 - 1,\ 0 \leq y \leq \frac{d-2}{2}\}$, and $T_2 = \{(x + \frac{1}{2}) + (y + \frac{1}{2})\sqrt{3}i \mid 0 \leq x \leq d|\mu|^2 - 1,\ 0 \leq y \leq \frac{d-2}{2}\}$ then $T = T_1 \cup T_2$ is a C.R.S. (mod γ). (See Figure 1).

PROOF. It is a trivial matter to show that T is a subset of $Z(\omega)$. Suppose $\alpha_1, \alpha_2 \in T$ and $\alpha_1 \equiv \alpha_2 (\text{mod } \gamma)$ then there exists $\delta = a_2 + b_2\omega$ such that $\alpha_1 - \alpha_2 = \delta\gamma$.

If $\alpha_1 = x_1 + y_1\sqrt{3}i$ and $\alpha_2 = x_2 + y_2\sqrt{3}i$ then $y_1 - y_2 = \frac{d}{2}(a_1b_2 + b_1a_2 - b_1b_2)$ so that $\frac{d}{2}\Big|(y_1 - y_2)$. But, $|y_1 - y_2| < \frac{d}{2}$ so that $y_1 = y_2$ and $x_1 \equiv x_2 (\text{mod } \gamma)$, Since the smallest real number that γ divides is $d|\mu|^2$ and $|x_1 - x_2| < d|\mu|^2$, we have $x_1 = x_2$ and $\alpha_1 = \alpha_2$.

If α_1 and α_2 are both in T_2 the same argument will again show that $\alpha_1 = \alpha_2$.

If α_1 and α_2 are such that $\alpha_1 = x_1 + y_1\sqrt{3}i$ and $\alpha_2 = (x_2 + \frac{1}{2}) + (y_2 + \frac{1}{2})\sqrt{3}i$ then $d/2$ divides $(y_1 - (y_2 + \frac{1}{2}))$ which is impossible since $2|d$. Hence, no two distinct elements of T are congruent modulo γ.

Let $\alpha = x + y\omega$. Find q_1 and r_1 such that $y = dq_1 + r_1$ where $0 \le r_1 < d$. Since $d = (a, b)$, there exists u and v such that $au + bv = dq_1$. If $r_1 = 2n_1$ find q_2 and n_2 such that $x - n_1 - au - av + bu = d|\mu|^2q_2 + n_2$ where $0 \le n_2 < d|\mu|^2$. If $r_1 = 2n_1 + 1$ find q_2 and n_2 such that $0 \le n_2 < d|\mu|^2$ where $x - n_1 - 1 - au - av + bu = d|\mu|^2q_2 + n_2$. When $r_1 = 2n_1$, we find that

$$\begin{aligned}\alpha &= x + y\omega \\ &= d|\mu|^2q_2 + (v + u(1 + \omega))\gamma + n_2 + n_1\sqrt{3}i \\ &\equiv n_2 + n_1\sqrt{3}i \ (\text{mod } \gamma)\end{aligned}$$

so that α is congruent to an element of T_1. On the other hand, if $r_1 = 2n_1 + 1$, we find that

$$\begin{aligned}\alpha &= x + y\omega \\ &= d|\mu|^2q_2 + (v + u(1 + \omega))\gamma + (n_2 + \tfrac{1}{2}) + (n_1 + \tfrac{1}{2})\sqrt{3}i \\ &\equiv (n_2 + \tfrac{1}{2}) + (n_1 + \tfrac{1}{2})\sqrt{3}i (\text{mod } \gamma)\end{aligned}$$

so that α is congruent to an element of T_2. In either case, α is congruent to an element of T and T is a C.R.S. (mod γ).

THEOREM 2.2. If d is odd, $T_1 = \{x + y\sqrt{3}i | 0 \le x \le d|\mu|^2 - 1, 0 \le y \le \frac{d-1}{2}\}$, and $T_2 = \{(x + \frac{1}{2}) + (y + \frac{1}{2})\sqrt{3}i | 0 \le x \le d|\mu|^2 - 1, 0 \le y \le \frac{d-3}{2}\}$ then $T = T_1 \cup T_2$ is a C.R.S. (mod γ). (See Figure 2).

The proof of Theorem 2.2 is very similar to that of Theorem 2.1 and hence has been omitted. Furthermore, examining the results of Theorems 2.1 and 2.2, we see that the following is true.

COROLLARY 2.1. The cardinality of a C.R.S. (mod γ) is $|\gamma|^2$.

3. REPRESENTATION II. Let $\gamma = a + b\omega$. Let T_1 be the collection of points inside the rhombus ABCD whose vertices are respectively $(1 + \omega)\gamma/2$, $(1 - \omega)\gamma/2$, $(-1 - \omega)\gamma/2$, and $(-1 + \omega)\gamma/2$. Let T_2 be the collection of points on the half-open line segments $(\pm(-1 + \omega)\gamma/2, (-1 - \omega)\gamma/2)$.

THEOREM 3.1. Let $T = T_1 \cup T_2$ then T is a C.R.S. (mod γ). (See Figures 3, 4, 5).

PROOF. --If $\alpha_1 = a_1 + b_1\omega$ then

$$\frac{\alpha_1}{\gamma} + \frac{1 + \omega}{2} = \left(\frac{a_1a - a_1b + b_1b}{N(\gamma)} + \frac{1}{2}\right) + \left(\frac{ab_1 - a_1b}{N(\gamma)} + \frac{1}{2}\right)\omega.$$

Let $C_1 = (a_1a - a_1b + b_1b)/N(\gamma)$, $D_1 = (ab_1 - a_1b)/N(\gamma)$, $r_1 = [C_1 + \frac{1}{2}]$, $R_1 = C_1 - r_1$, $s_1 = [D_1 + \frac{1}{2}]$, $S_1 = D_1 - s_1$ where [ ] is the greatest integer function then $C_1 + D_1\omega = \alpha_1/\gamma = (r_1 + s_1\omega) + (R_1 + S_1\omega)$ where $-\frac{1}{2} \leq R_1 < \frac{1}{2}$ and $-\frac{1}{2} \leq S_1 < \frac{1}{2}$. Hence, $\alpha_1 = (r_1 + s_1\omega)\gamma + (R_1 + S_1\omega)\gamma$ so that

$(R_1 + S_1\omega)\gamma \in Z(\omega)$ and $\alpha_1 \equiv (R_1 + S_1\omega)\gamma \pmod{\gamma}$.

For each of the following; CASE 1. $a + b \neq 0$, $2a - b \neq 0$, CASE 2. $a + b = 0$, $2a - b \neq 0$, and CASE 3. $a + b \neq 0$, $2a - b = 0$: it can be shown by using the equations for the sides of the rhombus that $(R_1 + S_1\omega)\gamma$ is in T_1 if R_1 and S_1 are in the open interval $(-\frac{1}{2}, \frac{1}{2})$ and $(R_1 + S_1\omega)\gamma$ is in T_2 if eigher P_1 or S_1 is equal to $-\frac{1}{2}$. Hence, every element of $Z(\omega)$ is congruent to some element of T.

Using the equations for the sides of ABCD, it can be shown that if $\alpha_1 \in T$ then $r_1 = s_1 = 0$.

Let α_1, $\alpha_2 \in T$ be such that $\alpha_1 \equiv \alpha_2 \pmod{\gamma}$ then there exists $\delta = a_3 + b_3\omega$ such that $\alpha_1/\gamma = \alpha_2/\gamma + \delta$. However, $\alpha_1 = (R_1 + S_1\omega)\gamma$ and $\alpha_2 = (R_2 + S_2\omega)\gamma$ where $-\frac{1}{2} \leq R_j$, $S_j < \frac{1}{2}$ for $j = 1, 2$ so that $(R_1 - R_2) + (S_1 - S_2)\omega = a_3 + b_3\omega$. Therefore, $R_1 - R_2 = a_3$ and $S_1 - S_2 = b_3$. Considering the possible values for R_j and S_j for $j = 1, 2$, and using the fact that a_3 and b_3 are integers, we have $a_3 = b_3 = 0$ or $\alpha_1 = \alpha_2$ so that T is a C.R.S. $\pmod{\gamma}$.

It is interesting to observe when T_2 is empty. To do this, we first note that the following is true.

THEOREM 3.2. If $\gamma = a + b\omega$ then $2|N(\gamma)$ iff $2|\gamma$.

We are now able to show

THEOREM 3.3. Let $\gamma = a + b\omega$ and $T = T_1 \cup T_2$. The set T_2 is empty iff $2\nmid\gamma$.

PROOF. --Let $\alpha_1 = a_1 + b_1\omega$. CASE 1. $a + b \neq 0$ and $2a - b \neq 0$. If α_1 is on CD then $N(\gamma) = 2(a_1b - a_1a - b_1b)$ while $N(\gamma) = 2(a_1b - ab_1)$ if α_1 is on BC. CASE 2. $a + b = 0$ and $2a - b \neq 0$. If α_1 is on CD then $N(\gamma) = 3a^2 = 2a(b_1 - 2a_1)$ whereas α_1 on BC implies that $N(\gamma) = 2(a_1b - ab_1)$. CASE 3. $a + b \neq 0$ and $2a - b = 0$. If α_1 is on CD then $N(\gamma) = 2(a_1b - a_1a - b_1b)$ and $N(\gamma) = 2a(2a_1 - b_1)$ if α_1 is on BC. Therefore, $T_2 \neq \phi$ implies that $2|\gamma$.

Conversely, it is easy to see that if $2|\gamma$ then the vertex C of the rhombus is a point of T_2 since the value of C_1 in Theorem 3.1 is $-\frac{1}{2}$.

4. <u>REPRESENTATION III</u>. In Hardman and Jordan (1) and Potratz (3) we find a discussion of a "better" or "absolute minimal representation" of a C.R.S. $\pmod{\gamma}$. For consistency, we have

DEFINITION 4.1. A representation T of a C.R.S. $\pmod{\gamma}$ is said to be an absolute minimal representation iff for any representation R of a C.R.S. $\pmod{\gamma}$, we have

$$\sum_{\alpha\in T} |\alpha| \leq \sum_{\beta\in R} |\beta|.$$

It is the purpose of this section to exhibit a representation of a C.R.S. (mod γ) which is a "better" or "absolute minimal representation". As before, we let $\gamma = a + b\omega$.

Let T_1 be the set of points interior to the hexagon ABCDEF whose vertices are given respectively by $\frac{\gamma}{3}(1 - \omega)e^{\pi ki/3}$ where $1 \le k \le 6$. Let T_2 be the set of points on the line segments $[-\frac{\gamma}{3}(1 - \omega), \frac{\gamma}{3}(1 - \omega)e^{4\pi i/3}]$, $[\frac{\gamma}{3}(1 - \omega)e^{4\pi i/3}, \frac{\gamma}{3}(1 - \omega)e^{5\pi i/3}]$ and $[\frac{\gamma}{3}(1 - \omega)e^{5\pi i/3}, \frac{\gamma}{3}(1 - \omega))$. Let $T = T_1 \cup T_2$.

THEOREM 4.1. The set T described above is a C.R.S. (mod γ). (See Figures 6, 7, 8, 9).

PROOF. Let $\alpha_1 = a_1 + b_1\omega$. In Theorem 3.1, it was shown that there exist integers r_1 and s_1 together with rationals R_1 and S_1 such that

$$\alpha_1/\gamma = (r_1 + s_1\omega) + (R_1 + S_1\omega)$$

where $-1 \le 2R_1 < 1$ and $-1 \le 2S_1 < 1$. Consider the follwoing cases: CASE 1. $-1 \le 2R_1 \le 0$ and $-1 \le 2S_1 \le 0$, CASE 2. $-1 \le 2R_1 \le 0$ and $0 < 2S_1 < 1$, CASE 3. $0 < 2R_1 < 1$ and $-1 \le 2S_1 \le 0$, and CASE 4. $0 < 2R_1 < 1$ and $0 < 2S_1 < 1$. It can be shown in each case that there exist integers r and s together with rationals R and S such that

$$\alpha_1/\gamma = (r + s\omega) + (R + S\omega)$$

where (1) $-1 \le R + S < 1$, (2) $-1 < R - 2S \le 1$, and (3) $-1 < S - 2R \le 1$. We shall say that a number in this form is in standard form. Note that $(R + S\omega)\gamma$ is an element of $Z(\omega)$ and that $\alpha_1 \equiv (R + S\omega)\gamma \pmod{\gamma}$.

Let us now consider the following possibilities for γ: CASE 1. $a \ne 0$, $b \ne 0$, and $a \ne b$, CASE 2. $a = 0$ and $b \ne 0$, CASE 3. $a \ne 0$ and $b = 0$, and CASE 4. $a \ne 0$, $b \ne 0$, and $a = b$. As in the proof of Theorem 3.1, if we use the equations for the sides of the hexagon together with the restrictions placed on a number α_1 in standard form we find in each case that $(R + S\omega)\gamma \in T$ and in particular that it is on DE if $R + S = -1$, on CD if $S - 2R = 1$, and on EF if $R - 2S = 1$. Therefore, every element of $z(\omega)$ is congruent to some element of T.

Let $\alpha_1 \varepsilon T$ in standard form. Since α_1 is between AB and DE, we have $r + s = -1$, $r + s = 0$, or $r + s = 1$. Similarly, $r - 2s$ equals -1, 0, or 1 since α_1 is between BC and EF while $s - 2r$ equals 1, 0, or -1 since α_1 is between CD and FA. Examining the twenty-seven possibilities, it is easy to see that all cases lead to a contradiction except where $r + s = 0$, $2r - s = 0$, and $r - 2s = 0$. Hence, $r = s = 0$ and $\alpha_1 = (R + S\omega)\gamma$.

Suppose α_1, $\alpha_2 \varepsilon T$ in standard form where $\alpha_1 = (R + S\omega)\gamma$ and $\alpha_2 = (U + V\omega)\gamma$. If $\alpha_1 \equiv \alpha_2 \pmod{\gamma}$ then there exists a δ such that $\alpha_1 - \alpha_2 = \gamma\delta$. Using the standard form restrictions, it can be shown that $\delta = \pm 1 \pm \omega$, $\pm\omega$, ± 1, or 0. However, $\alpha_2 + \gamma\delta = \alpha_1$ is not solvable in T for these δ's unless $\delta = 0$; therefore, any two distinct elements are incongruent modulo γ and T is a C.R.S. modulo γ.

In a paper to follow, the author will investigate necessary and sufficient conditions for the boundary of the complete residue system to be empty.

LEMMA 4.1. If $-1 \leq a < 1$ or $-1 < a \leq 1$ and r is any integer then $0 \leq r^2 + ar$.

The proof of Lemma 4.1 is straight forward and hence the details have been omitted.

LEMMA 4.2. Let $\alpha \varepsilon T$ then $|\alpha| \leq |\beta|$ for all $\beta \equiv \alpha \pmod{\gamma}$.

PROOF. Let $\alpha/\gamma = R + S\omega$ be in standard form. Now, $\beta = \alpha + \delta\gamma$ for some δ; therefore $\beta/\gamma = (R + S\omega) + (c + d\omega)$ where c and d are integers. Hence,

$$|\beta/\gamma| = \left[(R + c)^2 - (R + c)(S + d) + (S + d)^2\right]^{\frac{1}{2}}$$

$$= \left[2Rc - cS + c^2 - cd + 2Sd - Rd + d^2 + |\alpha/\gamma|^2\right]^{\frac{1}{2}}$$

$$= \left[D + |\alpha/\gamma|^2\right]^{\frac{1}{2}}$$

Suppose $c = d$ then $D = Rd + Sd + d^2 = d^2 + d(R + S) \geq 0$. If $c > d$ and $c < 0$ then $-c - 1 \leq 2S - R - c < 1 - c \leq -d$ or $-d^2 \geq (2S - R - c)d$. Therefore, $D = d^2 + d(2S - R - c) + c^2 + c(2R - S) \geq 0$. If $c > d$ and $c = 0$ then we have $D = d^2 + d(2S - R) \geq 0$. If $c > d$ and $c > 0$ then $-c \leq -d - 1 \leq 2R - S - d < 1 - d$ or $(2R - S - d)c + c^2 \geq 0$. Hence, $D = c^2 + c(2R - S - d) + d^2 + d(2S - R) \geq 0$. Similarly, $D \geq 0$ if $c < d$ and either $c = 0$, $c > 0$ or $c < 0$. Hence, $|\alpha| \leq |\beta|$.

That T is an absolute minimal representation of a C.R.S. (mod γ) is an immediate consequence of Lemma 4.2.

REFERENCES

1. Hardman, N. R. and J. H. Jordan. A Minimum Problem Connected with Complete Residue Systems in the Gaussian Integers, Amer. Math. Monthly 74 (1967) 559-561, No. 5.

2. Jordan, J. H. and C. J. Potratz. Complete Residue Systems in the Gaussian Integers, Math. Mag. 38 (1965) 1-12.

3. Potratz, C. J. Character Sums in $Z(\sqrt{-2})/(p)$. Unpublished Ph.D. dissertation, Washington State University, 1966.

4. Uspensky, J. V. and M. A. Heaslet. Elementary Number Theory, McGraw-Hill, New York, 1939.

KEY WORDS AND PHRASES. *Complete Residue Systems, Representations of Complete Residue Systems.*

AMS(MOS) SUBJECT CLASSIFICATIONS (1970). *12F05.*

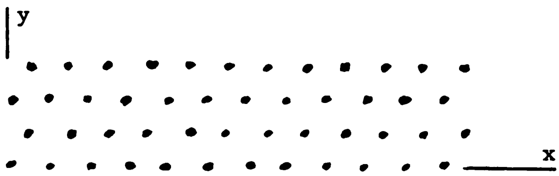

FIG. 1 C.R.S. (mod $4 + 8\omega$)

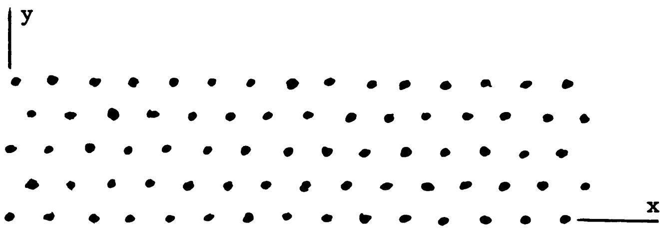

FIG. 2 C.R.S. (mod $5 + 10\omega$)

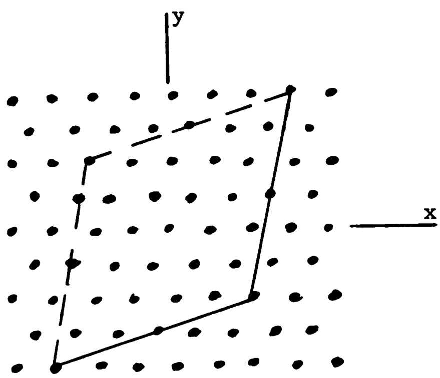

FIG. 3 C.R.S. (mod $4 + 6\omega$)

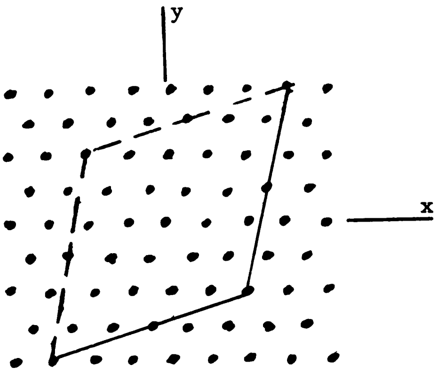

FIG. 4 C.R.S. (mod 7 - 7ω)

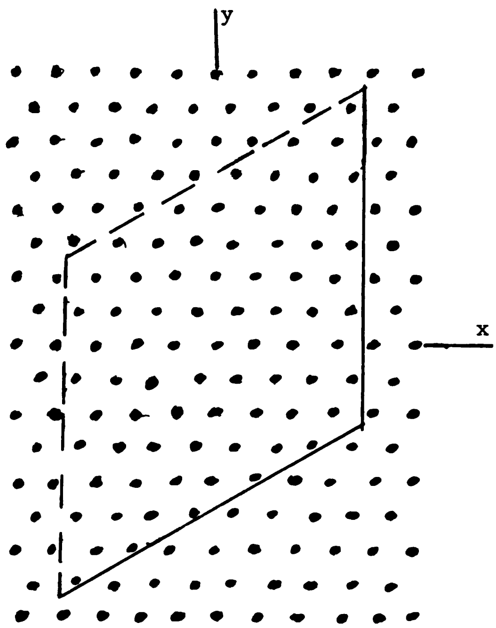

FIG. 5 C.R.S. (mod 5 + 10ω)

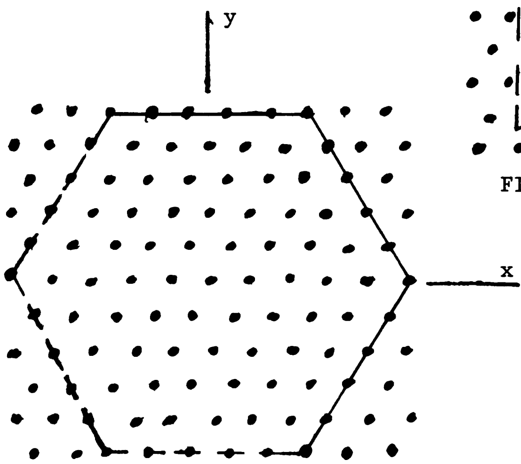

FIG. 6 C.R.S. (mod 5 + 10ω)

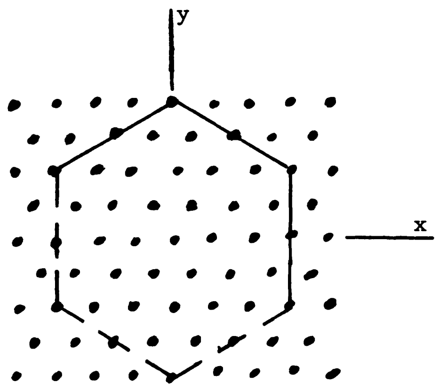

FIG. 7 C.R.S. (mod 6ω)

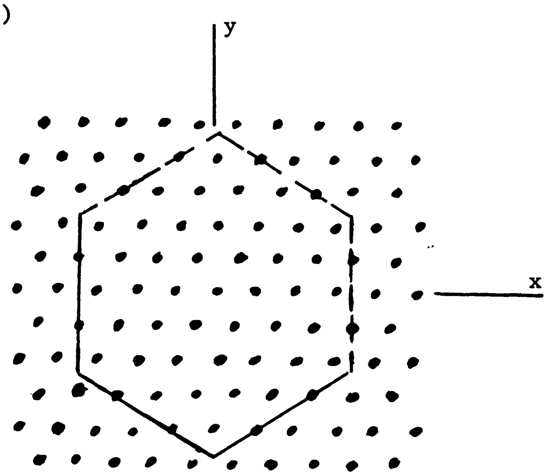

FIG. 8 C.R.S. (mod 7)

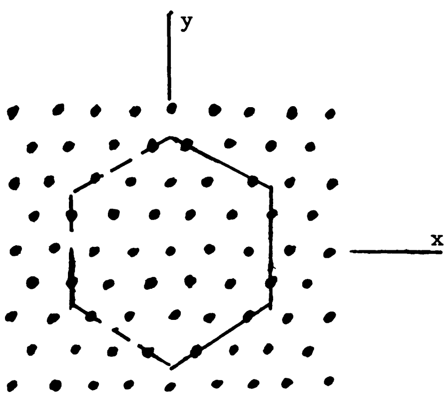

FIG. 9 C.R.S. (mod 5 + 5ω)