Proof. The proof follows the outline of Theorem 1. It should be noted in conclusion that if the ring is Boolean then each $x_{p_n}=0$ for all $p=1, 2, \cdots, m$ and the function reduces to the Boolean function as given in [2].

References

1. A. L. Foster, The theory of Boolean-like rings, Trans. Amer. Math. Soc., 59 (1946) 166–187.
2. F. E. Hohn, Applied Boolean Algebra: An Elementary Introduction, Macmillan, New York, 1960.

ON THE NUMBER OF SOLUTIONS OF A CONGRUENCE

K. S. WILLIAMS, University of Toronto

1. Notation. Let p be a prime, $p\equiv 1 \pmod 3$. Then the pair of integers A and B are uniquely determined by the relations:

$$4p = A^2 + 27B^2 \qquad A \equiv 1 \pmod 3, \quad B > 0.$$

We shall write $\theta_1=\frac{1}{2}(A+3B\sqrt{-3})$, $\theta_2=\bar{\theta}_1$ so $\theta_1\theta_2=p$. The complex cube roots of unity will be written w and w^2, where $w=\frac{1}{2}(-1+\sqrt{-3})$. Further the principal character (mod p) will be denoted by χ_0 and the two nonprincipal cubic ones by χ_1 and χ_2. In order to distinguish between these we have:

$$\chi_1(\alpha) = 1, w, w^2 \text{ according as } \alpha^{(p-1)/3} \equiv 1, w, w^2 \pmod{\theta_1}$$

$$\chi_2(\alpha) = 1, w^2, w \text{ according as } \alpha^{(p-1)/3} \equiv 1, w, w^2 \pmod{\theta_1}.$$

Hence we have $\chi_1^2=\chi_2$, $\chi_2^2=\chi_1$ and $\chi_1\chi_2=\chi_0$. Finally we write $e(t)$ for $\exp(2\pi it p^{-1})$ and define $\tau_i(\alpha)(i=1, 2)$ by

$$\tau_i(\alpha) = \sum_{x=1}^{p-1} \chi_i(x)e(\alpha x)$$

with $\tau_i=\tau_i(1)$. So we have the following relations

$$\tau_1\tau_2 = p, \qquad \tau_1^3 = p\theta_1, \qquad \tau_2^3 = p\theta_2 \tag{1.1}$$

and $\tau_1(\alpha)=\chi_2(\alpha)\tau_1$, $\tau_2(\alpha)=\chi_1(\alpha)\tau_2$.

2. Introduction. The above notation is essentially that used by Eckford Cohen in [1]. We shall find in this article an expression for the number of solutions N_n of the congruence:

$$a_1x_1^3 + a_2x_2^3 + \cdots + a_nx_n^3 + b \equiv 0 \pmod p, \quad \text{where} \quad p\nmid \prod_{i=1}^{n} a_i.$$

3. We first need a simple lemma.

LEMMA. *If* $p\nmid a$ *then* $\sum_{x=0}^{p-1} e(ax^3)=\tau_2\chi_1(a)+\tau_1\chi_2(a)$.

Proof.

$$\sum_{x=0}^{p-1} e(ax^3) = 1 + \sum_{y=1}^{p-1} e(ay)N(x: x^3 \equiv y) = 1 + \sum_{y=1}^{p-1} e(ay)[\chi_0(y) + \chi_1(y) + \chi_2(y)]$$
$$= \tau_1(a) + \tau_2(a) = \tau_1\chi_2(a) + \tau_2\chi_1(a) \qquad \text{using (1.1).}$$

4. Now

$$N_n = \frac{1}{p} \sum_{t=0}^{p-1} \sum_{x_1=0}^{p-1} \cdots \sum_{x_n=0}^{p-1} e\{t(a_1x_1^3 + \cdots + a_nx_n^3 + b)\}$$
$$= p^{n-1} + \frac{1}{p} \sum_{t=1}^{p-1} e(bt) \left\{ \sum_{x_1=0}^{p-1} e(a_1tx_1^3) \right\} \cdots \left\{ \sum_{x_n=0}^{p-1} e(a_ntx_n^3) \right\}$$
$$= p^{n-1} + \frac{1}{p} \sum_{t=1}^{p-1} e(bt)\{\tau_2\chi_1(a_1t) + \tau_1\chi_2(a_1t)\} \cdots \{\tau_2\chi_1(a_nt) + \tau_1\chi_2(a_nt)\}$$

using the lemma.

Now set

$$u_i = \tau_2\chi_1(a_i), \qquad v_i = \tau_1\chi_2(a_i) \qquad \text{for } i = 1, 2, \cdots, n. \tag{4.1}$$

Therefore

$$N_n = p^{n-1} + \frac{1}{p} \sum_{t=1}^{p-1} e(bt) \prod_{i=1}^{n} (u_i\chi_1(t) + v_i\chi_2(t)).$$

Define $x_n \equiv x_n(u_1, u_2, \cdots, u_n; v_1, v_2, \cdots, v_n) \equiv x_n(\underline{u}^{(n)}, \underline{v}^{(n)})$, similarly define y_n, z_n (noting that $x_n(\underline{v}^{(n)}, \underline{u}^{(n)})$ denotes $x_n(\underline{u}^{(n)}, \underline{v}^{(n)})$, where u_i has been replaced by v_i $(i=1, 2, \cdots, n)$ and vice-versa) by

$$x_n\chi_0(t) + y_n\chi_1(t) + z_n\chi_2(t) = \prod_{i=1}^{n} (u_i\chi_1(t) + v_i\chi_2(t)).$$

Thus

$$N_n = p^{n-1} + \frac{1}{p} \sum_{t=1}^{p-1} e(bt)[x_n\chi_0(t) + y_n\chi_1(t) + z_n\chi_2(t)].$$

Therefore,

$$N_n = p^{n-1} + \frac{x_n}{p}(p-1) \qquad \text{if } b \equiv 0 \pmod{p} \tag{4.2}$$

or

$$N_n = p^{n-1} - \frac{x_n}{p} + \frac{y_n}{p}\chi_2(b)\tau_1 + \frac{z_n}{p}\chi_1(b)\tau_2 \qquad \text{if } b \not\equiv 0 \pmod{p}. \tag{4.3}$$

5. We now define a symbol $[m, n-m]$ in terms of which we shall give x_n, y_n, z_n.

DEFINITION. *Let m and n be fixed integers such that $0 \leqq m \leqq n$. Define $[m, n-m]$ to be $\sum u \cdots uv \cdots v$, where there are m u's and $(n-m)$ v's and the subscripts in some order form the sequence $1, 2, \cdots, n$. In all there will be $\binom{n}{m}$ terms.*

EXAMPLES: $[0, 3] = v_1v_2v_3$, $[2, 1] = u_1u_2v_3 + u_1v_2u_3 + v_1u_2u_3$.

We understand $[0, 0]$ to mean 1. We thus have the following identity:

$$u_{n+1}[m, n-m] + v_{n+1}[m+1, n-m-1] = [m+1, n-m]. \tag{5.1}$$

6. Now

$$\begin{aligned} &x_n\chi_0(t) + y_n\chi_1(t) + z_n\chi_2(t) \\ &\quad = (u_n\chi_1(t) + v_n\chi_2(t))(x_{n-1}\chi_0(t) + y_{n-1}\chi_1(t) + z_{n-1}\chi_2(t)) \\ &\quad = (v_ny_{n-1} + u_nz_{n-1})\chi_0(t) + (u_nx_{n-1} + v_nz_{n-1})\chi_1(t) + (v_nx_{n-1} + u_ny_{n-1})\chi_2(t). \end{aligned}$$

Thus

$$\begin{aligned} x_n(\underline{u}^{(n)}, \underline{v}^{(n)}) &= v_ny_{n-1}(\underline{u}^{(n-1)}, \underline{v}^{(n-1)}) + u_nz_{n-1}(\underline{u}^{(n-1)}, \underline{v}^{(n-1)}) \\ y_n(\underline{u}^{(n)}, \underline{v}^{(n)}) &= u_nx_{n-1}(\underline{u}^{(n-1)}, \underline{v}^{(n-1)}) + v_nz_{n-1}(\underline{u}^{(n-1)}, \underline{v}^{(n-1)}) \\ z_n(\underline{u}^{(n)}, \underline{v}^{(n)}) &= v_nx_{n-1}(\underline{u}^{(n-1)}, \underline{v}^{(n-1)}) + u_ny_{n-1}(\underline{u}^{(n-1)}, \underline{v}^{(n-1)}). \end{aligned}$$

For completeness we define $x_0 = 1$; $y_0 = 0$; $z_0 = 0$. It is straightforward to show by induction that x_n is symmetric; that is,

$$x_n(\underline{u}^{(n)}, \underline{v}^{(n)}) = x_n(\underline{v}^{(n)}, \underline{u}^{(n)}).$$

It then follows immediately that $y_n(\underline{u}^{(n)}, \underline{v}^{(n)}) = z_n(\underline{v}^{(n)}, \underline{u}^{(n)})$. Now the difference equations simplify and we obtain

$$x_n(\underline{u}^{(n)}, \underline{v}^{(n)}) = v_ny_{n-1}(\underline{u}^{(n-1)}, \underline{v}^{(n-1)}) + u_ny_{n-1}(\underline{v}^{(n-1)}, \underline{u}^{(n-1)}), \tag{6.1}$$

$$\begin{aligned} y_n(\underline{u}^{(n)}, \underline{v}^{(n)}) = {} & u_nv_{n-1}y_{n-2}(\underline{u}^{(n-2)}, \underline{v}^{(n-2)}) + u_nu_{n-1}y_{n-2}(\underline{v}^{(n-2)}, \underline{u}^{(n-2)}) \\ & + v_ny_{n-1}(\underline{v}^{(n-1)}, \underline{u}^{(n-1)}), \end{aligned} \tag{6.2}$$

$$z_n(\underline{u}^{(n)}, \underline{v}^{(n)}) = y_n(\underline{v}^{(n)}, \underline{u}^{(n)}). \tag{6.3}$$

7. Let us define for convenience: $t = [m/6]$,

$$\begin{aligned} f(m) &= 1 \quad m \equiv 1, 4 \pmod 6 \\ &= 0 \quad m \equiv 0, 2, 3, 5 \pmod 6 \\ g(m) &= 1 \quad m \equiv 0, 1, 2 \pmod 6 \\ &= 0 \quad m \equiv 3, 4, 5 \pmod 6 \\ h(m) &= 0 \quad m \equiv 0 \pmod 3 \\ &= 2 \quad m \equiv 1 \pmod 3 \\ &= 1 \quad m \equiv 2 \pmod 3. \end{aligned}$$

Now we show that the solution of the difference equations is given by

$$x_m = \sum_{l=0}^{t-f(m)} [3l + h(m), m - 3l - h(m)] + \sum_{l=0}^{t-g(m)} [m - 3l - h(m), 3l + h(m)], \tag{7.1}$$

$$\begin{aligned} y_m = &\sum_{l=0}^{t-f(m+1)} [3l + h(m-2), m - 3l - h(m-2)] \\ &+ \sum_{l=0}^{t-g(m)} [m - 3l - h(m-1), 3l + h(m-1)], \end{aligned} \tag{7.2}$$

$$\begin{aligned} z_m = &\sum_{l=0}^{t-g(m)} [3l + h(m-1), m - 3l - h(m-1)] \\ &+ \sum_{l=0}^{t-f(m+1)} [m - 3l - h(m-2), 3l + h(m-2)]. \end{aligned} \tag{7.3}$$

We begin the inductive proof. We assume that the expressions for the y_m are true for $m=0, 1, 2, \cdots, 6n-1$ and deduce that they are valid for $m=6n$, $6n+1, \cdots, 6n+5$. It is easily verified that they are indeed valid for $m=0$, 1, 2, 3, 4, 5. We illustrate the inductive step from $m=6n-1$ to $m=6n$. The rest are similar. From the recurrence relations (6.1) and (6.3) we then have x_n and z_n. Now from (6.2),

$$\begin{aligned} &y_{6n}(\underline{u}^{(6n)}, \underline{v}^{(6n)}) \\ &= u_{6n}v_{6n-1}y_{6n-2}(\underline{u}^{(6n-2)}, \underline{v}^{(6n-2)}) + u_{6n}u_{6n-1}y_{6n-2}(\underline{v}^{(6n-2)}, \underline{u}^{(6n-2)}) \\ &\quad + v_{6n}y_{6n-1}(\underline{v}^{(6n-1)}, \underline{u}^{(6n-1)}) \\ &= u_{6n}v_{6n-1}\sum_{l=0}^{n-1} [3l+1, 6n-3l-3] + u_{6n}v_{6n-1}\sum_{l=0}^{n-1} [6n-3l-2, 3l] \\ &\quad + u_{6n}u_{6n-1}\sum_{l=0}^{n-1} [3l, 6n-3l-2] + u_{6n}u_{6n-1}\sum_{l=0}^{n-1} [6n-3l-3, 3l+1] \\ &\quad + v_{6n}\sum_{l=0}^{n-1} [6n-3l-1, 3l] + v_{6n}\sum_{l=0}^{n-1} [3l+2, 6n-3l-3] \\ &= u_{6n}\sum_{l=0}^{n-1} \{u_{6n-1}[3l, 6n-3l-2] + v_{6n-1}[3l+1, 6n-3l-3]\} \\ &\quad + u_{6n}\sum_{l=0}^{n-1} \{u_{6n-1}[6n-3l-3, 3l+1] + v_{6n-1}[6n-3l-2, 3l]\} \\ &\quad + v_{6n}\sum_{l=0}^{n-1} [6n-3l-1, 3l] + v_{6n}\sum_{l=0}^{n-1} [3l+2, 6n-3l-3] \end{aligned}$$

$$= \sum_{l=0}^{n-1} \{u_{6n}[3l+1, 6n-3l-2] + v_{6n}[3l+2, 6n-3l-3]\}$$

$$+ \sum_{l=0}^{n-1} \{u_{6n}[6n-3l-2, 3l+1] + v_{6n}[6n-3l-1, 3l]\} \quad \text{using (5.1)}$$

$$= \sum_{l=0}^{n-1} [3l+2, 6n-3l-2] + \sum_{l=0}^{n-1} [6n-3l-1, 3l+1] \quad \text{using (5.1) again.}$$

This is correct since $t=n$, $f(m+1)=1$, $g(m)=1$, $h(m-1)=1$, $h(m-2)=2$. This completes the proof.

8. We now define a new symbol, similar to $[m, n-m]$, namely $[\chi_1(a: m)\chi_2(a: n-m)]$ for positive integers n, m such that $0 \leqq m \leqq n$. The explanation of this symbol is perhaps best illustrated by two examples:

Example (i)

$$[\chi_1(a:1)\chi_2(a:2)] = \chi_1(a_1)\chi_2(a_2a_3) + \chi_1(a_2)\chi_2(a_3a_1) + \chi_1(a_3)\chi_2(a_1a_2).$$

Example (ii)

$$[\chi_1(a:0)\chi_2(a:3)] = \chi_2(a_1a_2a_3).$$

In general there will be $\binom{n}{m}$ terms.

9. Conclusion. If $b \equiv 0 \pmod{p}$, using (1.1), (4.1), (4.2) and (7.1) we find that

$$N_n = p^{n-1} + \frac{(p-1)}{p}\left\{\tau_1^n \sum_{l=0}^{t-f(n)} \left(\frac{\theta_2}{\theta_1}\right)^l \left(\frac{\tau_2}{\tau_1}\right)^{h(n)} [\chi_1(a:3l+h(n))\chi_2(a:n-3l-h(n))]\right.$$

$$\left. + \tau_2^n \sum_{l=0}^{t-g(n)} \left(\frac{\theta_1}{\theta_2}\right)^l \left(\frac{\tau_1}{\tau_2}\right)^{h(n)} [\chi_1(a:n-3l-h(n))\chi_2(a:3l+h(n))]\right\}.$$

In particular for $n=1, 2, 3$ we have the familiar results:

$$N_1 = 1,$$
$$N_2 = p + (p-1)(\chi_1(a_1)\chi_2(a_2) + \chi_1(a_2)\chi_2(a_1)),$$
$$N_3 = p^2 + (p-1)(\theta_2\chi_1(a_1a_2a_3) + \theta_1\chi_2(a_1a_2a_3)).$$

If $a_i=1$ $(i=1, 2, \cdots, n)$ then the expression for N_n simplifies to

$$N_n = p^{n-1} + \frac{(p-1)}{3p}[(\tau_1+\tau_2)^n + (\omega\tau_1+\omega^2\tau_2)^n + (\omega^2\tau_1+\omega\tau_2)^n].$$

If $b \not\equiv 0 \pmod{p}$, using (1.1), (4.1), (4.3), (7.1), (7.2), (7.3) we have

$$N_n = p^{n-1}$$

$$+ \frac{\chi_1(b)}{\tau_1}\left\{\tau_1^n \sum_{l=0}^{t-g(n)} \left(\frac{\theta_2}{\theta_1}\right)^l \left(\frac{\tau_2}{\tau_1}\right)^{h(n-1)} [\chi_1(a:3l+h(n-1))\chi_2(a:n-3l-h(n-1))]\right.$$

$$+\tau_2^n \sum_{l=0}^{t-f(n+1)} \left(\frac{\theta_1}{\theta_2}\right)^l \left(\frac{\tau_1}{\tau_2}\right)^{h(n-2)} [\chi_1(a:n-3l-h(n-2))\chi_2(a:3l+h(n-2))]\Big\}$$

$$+\frac{\chi_2(b)}{\tau_2}\Big\{\tau_1^n \sum_{l=0}^{t-f(n+1)} \left(\frac{\theta_2}{\theta_1}\right)^l \left(\frac{\tau_2}{\tau_1}\right)^{h(n-2)} [\chi_1(a:3l+h(n-2))\chi_2(a:n-3l-h(n-2))]$$

$$+\tau_2^n \sum_{l=0}^{t-g(n)} \left(\frac{\theta_1}{\theta_2}\right)^l \left(\frac{\tau_1}{\tau_2}\right)^{h(n-1)} [\chi_1(a:n-3l-h(n-1))\chi_2(a:3l+h(n-1))]\Big\}$$

$$-\frac{1}{p}\Big\{\tau_1^n \sum_{l=0}^{t-f(n)} \left(\frac{\theta_2}{\theta_1}\right)^l \left(\frac{\tau_2}{\tau_1}\right)^{h(n)} [\chi_1(a:3l+h(n))\chi_2(a:n-3l-h(n))]$$

$$+\tau_2^n \sum_{l=0}^{t-g(n)} \left(\frac{\theta_1}{\theta_2}\right)^l \left(\frac{\tau_1}{\tau_2}\right)^{h(n)} [\chi_1(a:n-3l-h(n))\chi_2(a:3l+h(n))]\Big\}.$$

With $n=1, 2, 3$ we have the known results [2]:

$$N_1 = 1 + \chi_2(a_1)\chi_1(b) + \chi_1(a_1)\chi_2(b),$$

$$N_2 = p + \theta_2\chi_1(a_1a_2b) + \theta_1\chi_2(a_1a_2b) - \chi_1(a_1)\chi_2(a_2) - \chi_1(a_2)\chi_2(a_1),$$

$$N_3 = p^2 + p(\chi_1(a_1a_2)\chi_2(a_3b) + \chi_1(a_2a_3)\chi_2(a_1b) + \chi_1(a_3a_1)\chi_2(a_2b) + \chi_1(a_1b)\chi_2(a_2a_3) + \chi_1(a_2b)\chi_2(a_3a_1) + \chi_1(a_3b)\chi_2(a_1a_2)) - (\theta_2\chi_1(a_1a_2a_3) + \theta_1\chi_2(a_1a_2a_3)).$$

If $a_i=1$ $(i=1, 2, \cdots, n)$ the formula becomes:

$$N_n = p^{n-1} + \frac{\chi_1(b)}{3\tau_1}[(\tau_1+\tau_2)^n + \omega^2(\omega\tau_1+\omega^2\tau_2)^n + \omega(\omega^2\tau_1+\omega\tau_2)^n]$$

$$+\frac{\chi_2(b)}{3\tau_2}[(\tau_1+\tau_2)^n + \omega(\omega\tau_1+\omega^2\tau_2)^n + \omega^2(\omega^2\tau_1+\omega\tau_2)^n]$$

$$-\frac{1}{3p}[(\tau_1+\tau_2)^n + (\omega\tau_1+\omega^2\tau_2)^n + (\omega^2\tau_1+\omega\tau_2)^n].$$

The author wishes to thank Mr. C. F. Dunkl, now at the University of Wisconsin, for a lively and stimulating conversation in connection with this article.

References

1. Eckford Cohen, Representations by cubic congruences. Proc. Nat. Acad. Sci. vol. 39, no. 2, 119–121, Feb. 1953.

2. ———, The number of solutions of certain cubic congruences, Pacific Journal of Mathematics, vol. 5, Suppl. 2, 877–886, 1955.

Editorial Note: It has been brought to the attention of the editors by Dr. M. G. Beumer of the Hague, Netherlands, that the results in the paper by Q. A. M. M. Yahya "On the generalization of Hilbert's inequality," this MONTHLY, 72(1965) 518–520, are all contained in a paper by Fu Cheng Hsiang, "An inequality for finite sequences," Math. Scandinavica, 5(1957) 12–14.