On exceptional systems of random integers.

Peter Hilton Bruce Love Jean Pedersen

1 Background, notation and terminology.

We collect together here the concepts and results which we will need in the sequel; details and proofs are to be found in [HP 1, 2].

Let $X_1, X_2, \cdots, X_k$ be independently distributed random integer variables such that X_j takes values in the range $1 \leq X_j \leq n_j$ with equal likelihood. Let m be a fixed but arbitrary modulus. We refer to $(n_1, n_2, \cdots, n_k; m)$, abbreviated to $(\underline{n}, k; m)$, as a **system**. Let $0 \leq u \leq m-1$; then we say that the system $(\underline{n}, k; m)$ is u-**good**, abbreviated to

$$(\underline{n}, k; m) \in \mathcal{G}_u, \tag{1.1}$$

if

$$\text{prob } (\Sigma = \sum_{j=1}^{k} X_j \equiv u \bmod m) = \frac{1}{m} \tag{1.2}$$

If $u = 0$, we abbreviate **0-good** to **good** and then write

$$(\underline{n}, k; m) \in \mathcal{G}. \tag{1.3}$$

Let $f = f(\underline{n}, k)$ be the polynomial

$$f = \frac{x^k \prod_j (x^{n_j} - 1)}{(x-1)^k}. \tag{1.4}$$

Received by the editors August 1994
Communicated by A. Warrinier
AMS Mathematics Subject Classification : 62E99; 11A07.
Keywords : Random integers; frequency generating functions, residue; factor system; sporadic system.

Then f is the **frequency generating function** for Σ. Let $R_m : \mathbb{Z}[x] \to \mathbb{Z}[x]$ be reduction mod $(x^m - 1)$. Then $r = R_m(f)$ is the **residue (mod m) frequency generation function**, or **residue polynomial**. If

$$r = \sum_{u=0}^{m-1} r_u x^u, \tag{1.5}$$

then

Proposition 1.1 *$(\underline{n}, k; m) \in \mathcal{G}_u$ if and only if $r_u = \dfrac{n_1 n_2 \cdots n_k}{m}$.*

We say that the system $(\underline{n}, k; m)$ is **standard** if $(\underline{n}, k; m) \in \mathcal{G}_u$ for all u in $0 \le u \le 1$. Then (Theorem 1.3 of [HP2])

Theorem 1.2 *$(\underline{n}, k; m)$ is standard if and only if $m | n_j$ for some j in $1 \le j \le k$.*

If $(\underline{n}, k; m)$ is good but not standard we say that it is **sporadic**. We will be entirely interested in sporadic systems in this paper, since standard systems are completely understood. Of course, Proposition 1.1 immediately implies

Proposition 1.3 *If $(\underline{n}, k; m)$ is u-good for any u in $0 \le u \le m-1$, then $m | n_1 n_2 \cdots n_k$.*

We write $\underline{n} \equiv \underline{n}'$ mod m if $n_j \equiv n_j'$ mod m for all j in $1 \le j \le k$. Then (Theorem 1.4 of [HP2])

Theorem 1.4 *If $\underline{n} \equiv \underline{n}'$ mod m, then*

$$(\underline{n}, k; m) \in \mathcal{G}_u \Leftrightarrow (\underline{n}', k; m) \in \mathcal{G}_u$$

for any u in $0 \le u \le m-1$.

In the light of Theorem 1.4 we may henceforth always assume, in our search for sporadic systems, that

$$0 < n_j < m \text{ for all } j \text{ in } 1 \le j \le k. \tag{1.6}$$

Thus we will assume (1.6) throughout the rest of this paper. In [HP2] we found a systematic recipe for constructing sporadic systems. Let m admit the factorization

$$m = a_1 a_2 \cdots a_k, \tag{1.7}$$

where each a_j is strictly less than m; we will call this a **proper k-factorization** of m. We then set $n_j = m - a_j$ and call $(\underline{n}, k; m)$ a **factor system**.

Now given any system $(\underline{n}, k; m)$, set

$$\bar{u} = \sum_j n_j - (k-1)m + k. \tag{1.8}$$

Then $\bar{u} \leq m$, and $\bar{u} = m$ if and only if each $n_j = m - 1$. Of course, in the latter case, $(\underline{n}, k; m)$ cannot be u-good for any u, so we will exclude it henceforth. Thus we may conclude that

$$\bar{u} \leq m - 1. \tag{1.9}$$

Then the main theorem of [HP2] (actually expressed in Corollary 2.5 of that paper) is the following :

Theorem 1.5 *$(\underline{n}, k; m)$ is a factor system if and only if the following 2 conditions hold:*

$$(i)\ \bar{u} \geq 1; \quad (ii)\ (\underline{n}, k; m) \in \mathcal{G}.$$

Moreover, we then also have $(\underline{n}, k; m) \in \mathcal{G}_{\bar{u}}$.

It is thus natural to ask whether there are any sporadic systems which are not factor systems; equivalently, whether there are sporadic systems for which $\bar{u} \leq 0$. As we showed in [HP2], there are such systems. However we first give two results in the opposite direction. Recall that we are concerned only to detect sporadic (good) systems subject to condition (1.6).

First, from the complete analysis of the case $k = 2$ in [HP2] we easily infer

Theorem 1.6 *Let $k = 2$. Then $(\underline{n}, k; m)$ is good if and only if it is a factor system.*

Second, let us describe the system $(\underline{n}, k; m)$ as **homogeneous** if $n_1 = n_2 = \cdots = n_k =$, say, n. We will then write $(n; k; m)$ instead of $(\underline{n}, k; m)$. Theorem 3.1 of [HP1] immediately implies

Theorem 1.7 *Let $k = 3$. Then the homogeneous system $(n; k; m)$ is good if and only if it is a factor system.*

On the other hand, we gave two examples in [HP2] of families of inhomogeneous systems $(\underline{n}, 3; m)$ which are good but not factor systems. Thus Examples 4.1, 4.2 of [HP2] may be described as follows.

Theorem 1.8 *Let $d \geq 1$. Then the systems*

$$(d, d+1, d+2; 2d+4) \text{ and } (2, 2d-1, d+2; 2d+4)$$

are good. Of course, neither is a factor system – in fact, $\bar{u} = -d-2$ for each system.

That there are sporadic systems which are not factor systems for all $k \geq 3$ now follows from Theorem 4.3 of [HP2], namely,

Theorem 1.9 *Let $(\underline{n}, k; m)$ be a system and let $(\underline{n}^+, k+1; m)$ be formed from $(\underline{n}, k; m)$ by adjoining the component $m - 1$. Then $\bar{u}$ is unchanged in passing to the augmented system and $(\underline{n}, k; m)$ is u-good if and only if $(\underline{n}^+, k+1; m)$ is u-good, for any u in $0 \leq u \leq m - 1$.*

We will obtain in Section 2 a family of homogeneous sporadic systems which are not factor systems and which involve variable values of k; among these systems there will be, as special cases, homogeneous systems with $k = 4$, so that Theorem 1.7 fails for higher values of k. In Section 3 we will obtain a very general result which includes Theorem 1.8 and shows that, in fact, the two systems described in the statement of that theorem are at the two extremes of a family comprising the only possible examples of sporadic, non-factor systems of a certain type.

Although, as we have said, our main interest in this paper is in sporadic, that is, 0-good systems, we are obviously also concerned with u-good systems for values of $u \neq 0$. In an appendix (Section 4) we prove a theorem about the coefficients r_u of (1.5) which explains the final assertion of Theorem 1.5 and Proposition 2.3, and provides a supplement to Theorem 3.1.

We point out that the properties of the families described in Sections 2 and 3 were suspected as a result of computer experiments carried out to detect sporadic, non-factor systems. These experiments, which are described briefly in Appendix 2 (Section 5), have thrown up other examples which we have not yet succeeded in explaining.

2 On a family of homogeneous sporadic systems.

In this section s is an arbitrary *even* positive integer and v is an arbitrary *odd* positive integer.

Theorem 2.1 *The homogeneous system $(s; vs; 2s)$ is good.*

Note that $\bar{u} = s(v + 2 - vs)$. Thus the system $(s; vs; 2s)$ is a factor system only if $s = 2$, $v = 1$. Note also that $(4; 4; 8)$ constitutes a homogeneous sporadic system with $k = 4$ which is not a factor system.

Before proceeding with the proof, we state a preliminary lemma whose proof may be left to the reader. Recall that $p \in \mathbb{Z}[x]$ is **antisymmetric** if $p(x) = -x^d p(\frac{1}{x})$, where $d = \deg p$.

Lemma 2.2 *Given $a > b$, with a odd, b even, then*

$$\frac{(x^r - 1)^a}{(x - 1)^b}$$

is an antisymmetric polynomial of degree $ar - b$.

Proof of Theorem 2.1

Let

$$f = \frac{x^{vs}(x^s - 1)^{vs}}{(x - 1)^{vs}},$$

$$g = \frac{x^s(x^s - 1)^{vs}}{(x - 1)^{vs}},$$

$$h = \frac{(x^s-1)^{vs}}{(x-1)^{vs}},$$

Then f is the frequency generating function for the system $(s; vs; 2s)$. Moreover,

$$R_{2s}(f) = R_{2s}(g), \tag{2.1}$$

since $x^{2s} - 1 | f - g$; recall that v is odd. We must therefore show that

$$R_{2s}(g)(0) = \frac{1}{2}s^{vs-1}, \tag{2.2}$$

according to Proposition 1.1.

Let c_m be the (cyclotomic) polynomial

$$c_m = 1 + x + x^2 + \cdots + x^{m-1}.$$

Since $h = c_s^{vs}$ it follows that

$$h = q(x^s - 1) + \lambda c_s,$$

where $\lambda = \frac{h(1)}{s} = s^{vs-1}$. Thus

$$h = q(x^s - 1) + s^{vs-1}c_s, \tag{2.3}$$

whence

$$g + h = (x^s + 1)h = q(x^{2s} - 1) + s^{vs-1}c_{2s}. \tag{2.4}$$

It follows that

$$R_{2s}(g) + R_{2s}(h) = s^{vs-1}c_{2s}. \tag{2.5}$$

Now consider $g - h = \dfrac{(x^s-1)^{vs+1}}{(x-1)^{vs}}$. By Lemma 2.2, $g - h$ is an antisymmetric polynomial of degree $2st$, where $t = \frac{1}{2}vs - \frac{1}{2}(v-1)$. Let a_l be the coefficient of x^{2ls} in this polynomial, $l = 0, 1, \cdots, t$. Then

$$R_{2s}(g-h)(0) = \sum_{l=0}^{t} a_l.$$

However, by the antisymmetry of $g - h$,

$$a_l = -a_{t-l},$$

so that

$$R_{2s}(g-h)(0) = 0. \tag{2.6}$$

Moreover, $R_{2s}(g - h) = R_{2s}(g) - R_{2s}(h)$, so that

$$R_{2s}(g-h)(0) = R_{2s}(g)(0) - R_{2s}(h)(0);$$

thus

$$R_{2s}(g)(0) = R_{2s}(h)(0). \tag{2.7}$$

However, it follows immediately from (2.5) that

$$R_{2s}(g)(0) + R_{2s}(h)(0) = s^{vs-1}. \tag{2.8}$$

Of course, (2.7) and (2.8) together imply (2.2), so that the theorem is proved.

Remark Notice that $g = x^s h$. Thus

$$\text{if } R_{2s}(f) = \sum_{u=0}^{2s-1} r_u x^u, \text{ then } R_{2s}(g) = \sum_{u=0}^{2s-1} r_u x^u, \quad \text{by (2.1)},$$

and

$$R_{2s}(h) = \sum_{u=0}^{2s-1} r'_u x^u,$$

where

$$r'_u = \begin{cases} r_{s+u}, & 0 \le u \le s-1 \\ r_{-s+u}, & s \le u \le 2s-1 \end{cases} \tag{2.9}$$

Thus, by (2.5), the polynomial $R_{2s}(f)$ has the property

$$r_u + r_{s+u} = s^{vs-1}, \quad 0 \le u \le s-1. \tag{2.10}$$

In particular, since $r_0 = \frac{1}{2}s^{vs-1}$, it follows that $r_s = \frac{1}{2}s^{vs-1}$, so that we conclude

Proposition 2.3 *The homogeneous system $(s; vs; 2s)$ is s-good.*

Of course, we can use Theorem 1.9 to construct new sporadic systems which will fail to be factor systems except in the case $s = 2$, $v = 1$. However, the systems we construct in this way will not themselves be homogeneous.

3 On sporadic, non-factor systems.

In this section we prove a theorem which provides both a generalization and a converse of Theorem 1.8. We consider systems $(a, b, c; 2c)$, so that $k = 3$. We may assume, without loss of generality, that $a \le b$. It is easy to see that, if $(a, b, c; 2c)$ is a factor system, then $a = 2c - 2$, $b = 2c - 1$. We now assume that $(a, b, c; 2c)$ is *not* a factor system and prove

Theorem 3.1 *Assume $(a, b, c; 2c)$ is not a factor system. Then*

$$(a, b, c; 2c) \in \mathcal{G} \Leftrightarrow 2c = a + b + 3.$$

Proof We first show that

$$(a, b, c; 2c) \in \mathcal{G} \text{ and } a + b \le 2c - 1 \Leftrightarrow 2c = a + b + 3. \tag{3.1}$$

Now, since $a \le b$, the frequency generating function f is given by

$$f = (x^2+2x^3+\cdots+ax^{a+1}+\cdots ax^{b+1}+(a-1)x^{b+2}+\cdots+x^{a+b})(x+x^2+\cdots+x^c) \quad (3.2)$$

If $a+b<c$, then (in the notation of (1.5)) $r_0 = 0$, so $(a,b,c;2c) \notin \mathcal{G}$. If $c \leq a+b \leq 2c-1$, then r_0 is the coefficient of x^{2c} in (3.2). Moreover, $c \geq a+1$. If, further, $c \leq b+1$, then

$$r_0 = (b-c+2)a+1+2+\cdots+(a-1) = (b-c+2)a+\frac{a(a-1)}{2}.$$

Thus

$$(a,b,c;2c) \in \mathcal{G} \Leftrightarrow r_0 = \frac{ab}{2} \Leftrightarrow 2b-2c+4+a-1 = b \Leftrightarrow 2c = a+b+3 \qquad (3.3)$$

Now suppose $c \leq a+b \leq 2c-1$ and $c > b+1$. Then, from (3.2)

$$r_0 = 1+2+\cdots+(a+b+1-c) = \frac{1}{2}(a+b+1-c)(a+b+2-c) \qquad (3.4)$$

But $a+b+1-c < a$, $a+b+2-c \leq a$, so, by (3.4), $r_0 < \frac{1}{2}a^2 \leq \frac{1}{2}ab$, whence $(a,b,c;2c) \notin \mathcal{G}$. We have proved that if $(a,b,c;2c) \in \mathcal{G}$ and $a+b \leq 2c-1$, then $c \leq b+1$, and $2c = a+b+3$. But, conversely, if $2c = a+b+3$, then, trivially, $a+b \leq 2c-1$ and $a<b$, since a,b have opposite parity. Thus $2c \leq 2b+2$, $c \leq b+1$, so that, by (3.3), $(a,b,c;2c) \in \mathcal{G}$. Thus (3.1) is proved.

Next we calculate $\bar{u}$, obtaining

$$\bar{u} = a+b+c-4c+3 = a+b-3c+3.$$

Thus

$$\bar{u} \geq 1 \Leftrightarrow a+b \geq 3c-2. \qquad (3.5)$$

It thus follows from Theorem 1.5 that if $a+b \geq 3c-2$ and $(a,b,c;2c) \in \mathcal{G}$ then $(a,b,c;2c)$ is a factor system, contrary to hypothesis. The proof of the theorem will therefore be completed when we have shown that

$$2c \leq a+b < 3c-2 \Rightarrow (a,b,c;2c) \notin \mathcal{G}. \qquad (3.6)$$

We divide the proof of (3.6) into 2 cases, as follows.

Case 1: $a < c \leq b$

It follows from the fact that $a+b < 3c-2$ that to calculate r_0 we again seek the coefficient of x^{2c} in (3.2). Thus

$$r_0 = (b-c+2)a+(a-1)+\cdots+(a+b+2-2c) = (b-c+2)a+\frac{1}{2}(2c-b-2)(2a+b+1-2c).$$

Trivial algebraic manipulation[1] now tells us that

$$2(r_0 - \frac{1}{2}ab) = (2c-b)(a+b-2c+3)-2.$$

[1] Not trivial, however, to a computer endowed with the capacity for symbolic manipulation!

But $2c-b \geq 1$, by our assumption (1.6), and $a+b-2c+3 \geq 3$, so $2(r_0 - \frac{1}{2}ab) \geq 1$, and hence $r_0 \neq \frac{1}{2}ab$. Equivalently, $(a,b,c;2c) \notin \mathcal{G}$.

Case 2: $c \leq a$

Again we seek the coefficient of x^{2c} in (3.2). Thus

$$r_0 = (c-1) + \cdots + (a-1) + (b-a+1)a + \frac{1}{2}(2c-b-2)(2a+b+1-2c)$$

– taking advantage of the calculation in Case 1.

Hence

$$\begin{aligned} r_0 &= \frac{1}{2}(a-c+1)(a+c-2) - (a-c+1)a + (b-c+2)a \\ &\qquad + \frac{1}{2}(2c-b-2)(2a+b+1-2c) \\ &= -\frac{1}{2}(a-c+1)(a-c+2) + (b-c+2)a + \frac{1}{2}(2c-b-2)(2a+b+1-2c). \end{aligned}$$

Again taking advantage of the calculation in Case 1, we conclude that

$$2(r_0 - \frac{1}{2}ab) = (2c-b)(a+b-2c+3) - 2 - (a-c+1)(a-c+2). \tag{3.7}$$

Now set $a-c+1 = q$. Then $q \geq 1$. Moreover,

$$2c-b > a-c+2 = q+1$$

and

$$a+b-2c+3-(a-c+1) = b-c+2 \geq 2,$$

so

$$a+b-2c+3 \geq q+2,$$

Thus, from (3.7),

$$2(r_0 - \frac{1}{2}ab) \geq (q+2)^2 - 2 - q(q+1) = 3q+2 \geq 5.$$

Certainly $r_0 \neq \frac{1}{2}ab$ and $(a,b,c;2c) \notin \mathcal{G}$. The proof of (3.6) is complete; and, with it, the proof of Theorem 3.1.

Remarks (i) Theorem 3.1 plainly incorporates Theorem 1.8, since it asserts that

$$(a,b,d+2;2d+4) \text{ is good provided } 2d+4 = a+b+3, a+b = 2d+1.$$

Except for the case $(1,2d,d+2;2d+4)$, the systems described in Theorem 1.8 are the extremal cases $a=2$, $a=d$. The exclusion of the case $a=1$ was due to a reluctance to admit 'dice with only one face' ![2] It is reasonable to have insisted that

[2] It is obvious that if $\bar{r}$ is the residue polynomial obtained by adjoining a 'die with only one face', then $\bar{r}_0 = r_{m-1}$, $\bar{r}_u = r_{u-1}$, $1 \leq u \leq m-1$. Thus the situation with $k=3$ and $n_1 = 1$ is immediately and entirely deducible from our complete analysis in [HP2] of the case $k=2$.

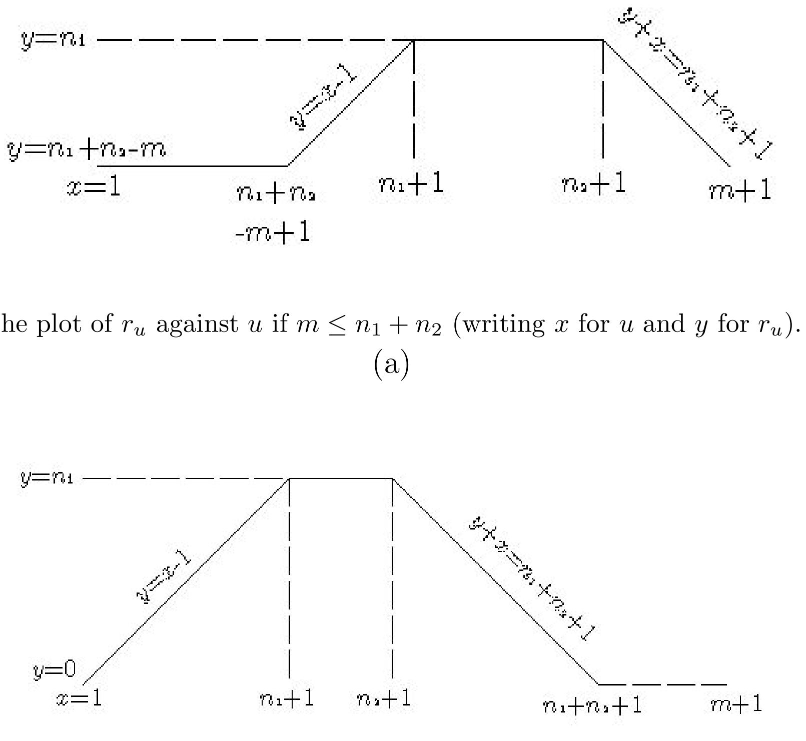
$d \geq 1$ (so that $c \geq 3$) in Theorem 1.8, since the equation $2c = a + b + 3$ implies $c \geq 3$.

(ii) Notice that it follows from Theorem 3.1 that if $(a, b, c; 2c)$ is good, then a, b have opposite parity. It is immediately plain from Proposition 1.1 that if $(a, b, c; 2c)$ is good then ab is even, but the stronger statement above is not at all obvious.

4 Appendix 1: On the shape of the residue coefficient curve.

In Proposition 2.3 we saw that $(s; vs; 2s)$ was not only good but also s-good. We also noted in the fundamental Theorem 1.5 that a factor system $(\underline{n}, k; m)$ is not only good but $\bar{u}$-good. In this appendix we will prove that, for *any* system $(\underline{n}, k; m)$, if it is good then it is also μ-good for a special μ in $0 \leq \mu \leq m - 1$.

We do this by studying the way the coefficients r_u of the residue frequency generating function $r = R_m(f)$ vary with u. This study was encapsulated, in the case $k = 2$, in Figure 1 of [HP2], and we will see that, in general, this variation was presaged in that figure, which we reproduce below.



The plot of r_u against u if $m \leq n_1 + n_2$ (writing x for u and y for r_u).

(a)

The plot of r_u against u if $m \geq n_1 + n_2$ (writing x for u and y for r_u).

(b)

(Figures (a) and (b) are drawn with the same value of n_1 and of n_2.)

Figure 1.

Given a system $(\underline{n}, k; m)$, we define μ to be the remainder when $\sum n_j + k$ is divided by m. We prove

Theorem 4.1 *In the residue polynomial* $r = \sum_{u=0}^{m-1} r_u x^u$ *we have*

$$r_u = r_{\mu-u}, \quad u = 0, 1, \cdots, \mu; \quad r_u = r_{m+\mu-u}, u = \mu+1, \mu+2, \cdots, m-1.$$

Proof We have

$$\frac{x^k \prod(x^{n_j}-1)}{(x-1)^k} = q(x)(x^m-1) + \sum_{u=0}^{\mu} r_u x^u + \sum_{u=\mu+1}^{m-1} r_u x^u. \tag{4.1}$$

Hence

$$\frac{x^{-k} \prod(x^{-n_j}-1)}{(x^{-1}-1)^k} = q(x^{-1})(x^{-m}-1) + \sum_{u=0}^{\mu} r_u x^{-u} + \sum_{u=\mu+1}^{m-1} r_u x^{-u}. \tag{4.2}$$

Notice that $q(x)$ is the zero polynomial if $\sum n_j < m$, and otherwise a polynomial of degree $\sum n_j - m$. We multiply through in (4.2) by $x^{\sum n_j + k}$, obtaining

$$\frac{x^k \prod(x^{n_j}-1)}{(x-1)^k} = -x^{\sum n_j+k-m} q(x^{-1})(x^m-1) + x^{\sum n_j+k-\mu} \sum_{u=0}^{\mu} r_u x^{\mu-u}$$

$$+x^{\sum n_j+k-\mu-m} \sum_{u=\mu+1}^{m-1} r_u x^{m+\mu-u} \tag{4.3}$$

Now $x^{\sum n_j+k-\mu} \equiv 1 \bmod (x^m-1)$ and $x^{\sum n_j+k-\mu-m} \equiv 1 \bmod (x^m-1)$.

Thus we deduce from (4.3) that, calculating mod (x^m-1),

$$\frac{x^k \prod(x^{n_j}-1)}{(x-1)^k} = \sum_{u=0}^{\mu} r_{\mu-u} x^u + \sum_{u=\mu+1}^{m-1} r_{m+\mu-u} x^u \tag{4.4}$$

Comparing (4.1) with (4.4), we deduce from the uniqueness of the remainder that

$$r_u = r_{\mu-u}, \quad u = 0, 1, \cdots, \mu; \quad r_u = r_{m+\mu-u}, u = \mu+1, \mu+2, \cdots, m-1.$$

Corollary 4.2 *Suppose that* $(\underline{n}, k; m)$ *is good. Then it is also* μ*-good.*

Notice that it is, of course, possible that $\mu = 0$, in which case Corollary 4.2 gives us no information. However, we may generalize Corollary 4.2 as follows: then even the case $\mu = 0$ is informative.

Theorem 4.3

$$(\underline{n}, k; m) \text{ is } \mu - \text{good} \Leftrightarrow (\underline{n}, k; m) \text{ is } (\mu - u) - \text{good}, \quad 0 \le u \le \mu$$

and

$$(\underline{n}, k; m) \text{ is } \mu - \text{good} \Leftrightarrow (\underline{n}, k; m) \text{ is } (m + \mu - u) - \text{good}, \quad \mu + 1 \le u \le m - 1.$$

Example 4.4 Suppose that $(\underline{n}, k; m)$ is a factor system. Then $1 \leq \bar{u} \leq m - 1$ where, by (1.8),

$$\bar{u} = \sum_j n_j - (k-1)m + k.$$

Thus $\bar{u} = \mu$, so that Corollary 4.2 yields the final statement of Theorem 1.5.

Example 4.5 We consider the homogeneous system $(s; vs; 2s)$ of Theorem 2.1. The remainder on dividing $vs^2 + vs$ (v odd, s even) by $2s$ is s. Thus, since $(s; vs; 2s)$ is good, we infer from Corollary 4.2 that $(s; vs; 2s)$ is s-good, as asserted in Proposition 2.3.

Example 4.6 We consider the sporadic system $(a, b, c; 2c)$ of Theorem 3.1 with $2c = a + b + 3$. The remainder on dividing $a + b + c + 3$ by $2c$, that is, $3c$ by $2c$, is c. Thus we infer from Corollary 4.2 that, if $2c = a + b + 3$, then the system $(a, b, c; 2c)$ is c -good.

Notice that, under the augmentation process described in Theorem 1.9, not only $\bar{u}$ but also μ remains unchanged. It would be interesting to study further the 'curve' r_u, that is, the dependence of r_u on u, in qualitative terms. It appears that we have a parabolic shape between $u = 0$ and $u = \mu$ and a second parabolic shape between $u = \mu + 1$ and $u = m - 1$. One of these parabolas, we believe, has a maximum and the other a minimum. We hope to revert to this matter in a later paper.

5 Appendix 2: How the computer data was obtained.

We include here a brief description of how Theorem 2.1 came to be conjectured.

Working with a Macintosh Centris 650, a program consisting of two levels was designed to generate solutions for the homogeneous case. The outer level was written in C and used nested loops which fed the inner level the number of dice (k) and the number of faces on each die (n). It also created an empty array (A) representing the frequency table for possible results of adding the values of k dice. This array was created for A_0 to A_{kn}, although the initial entries from A_0 to A_{k-1} were not used.

The inner loop was written in Assembler Language to maximize speed. Use was made of a 1-1-correspondence between the numbers 0 to $n^k - 1$ and the sum of the values on the dice using base n. A 32-bit register was used as the primary counter. Each value of this register was successively divided by n and the remainders accumulated. The final sum was adjusted to compensate for the faces of the dice being numbered from 1 to n, instead of (what is more natural in assembler language and in modular arithmetic) 0 to $n-1$. The frequency table was then incremented at the appropriate position. This method had the limitation that $n^k < 2^{32}$. However this limitation never became important because time to complete the simulation was a more limiting factor.

The final table was then passed back to the outer level. All multiples of the table's index were accumulated so that $r_m = \sum_j A_{mj}$. Then the program examined the table for values of m for which $mr_m = n^k$ and these were printed out.

The program was eventually changed, to accommodate the inhomogeneous case, using a formula to calculate values in the table rather than create them from scratch, with the arithmetic changed to work up to 64 bits. More data were created in the process, but no new phenomena were revealed.

References

[1] [HP1] Hilton, Peter, and Jean Pedersen, A conjecture on sums of random integers, **Bull. Soc. Math. Belg. 42** (Series B) (1990), 265 - 274.

[2] [HP2] Hilton, Peter, and Jean Pedersen, On residue classes of sums of random integers, **Bull. Soc. Math. Belg. 44** (Series B) (1992), 1 - 15.

Peter Hilton
Department of Mathematical Sciences
State University of New York
Binghamton, New York 13902-6000
U. S. A.

and
Department of Mathematics and Statistics
University of Otago
P. O. Box 56
Dunedin
New Zealand

Bruce Love
40 Mansel Avenue
Hamilton
New Zealand

Jean Pedersen
Department of Mathematics
Santa Clara University
Santa Clara, California 95053
U. S. A.

and
Department of Mathematics and Statistics
University of Otago
P. O. Box 56
Dunedin
New Zealand