ACTA ARITHMETICA
XXXVIII (1980)

Integers whose multiples have anomalous digital frequencies

by

KENNETH B. STOLARSKY (Urbana, Ill.)

1. Introduction. Let $B(n)$ be the number of ones in the binary expansion of n. For example, $B(37) = 3$ since $37 = 32+4+1$. Fix an integer $k > 1$. Numerical data indicates that if a large integer n is chosen "at random," then the difference $B(kn)-B(n)$ is just as likely to be negative as positive, and tends to be surprisingly small. On the other hand, there are presumably anomalous integers n such that $B(kn) \geqslant B(n)$ for *all* $k \geqslant 1$. We call such numbers *sturdy*. For example, the first 10 integers are sturdy, but $11 = 8+2+1$ is not, since $3\cdot 11 = 32+1$.

The question as to whether the sturdy numbers have zero density seems to be open, and rather difficult. Let $S(x)$ denote the number of integers less than or equal to x that are sturdy. We shall show that

$$S(x) > .5x^{1/2} \tag{1.1}$$

and

$$\liminf_{x\to\infty} S(x)/x \leqslant 1/2. \tag{1.2}$$

Inequality (1.1) is proved in Section 2. Inequality (1.2) is an immediate consequence of the fact (proved in Section 3) that the number of solutions of

$$B(3n)-B(n) = a, \quad 2^r \leqslant n < 2^{r+1} \tag{1.3}$$

is asymptotic to

$$(3/2\pi r)^{1/2}2^r\exp(-3a^2/2r) \tag{1.4}$$

for

$$|a| \leqslant r^{2/3-\varepsilon}, \quad \varepsilon > 0, \tag{1.5}$$

and is

$$O[r2^r \exp(-r^{1/3-2\varepsilon})] \tag{1.6}$$

for

$$|a| > r^{2/3-\varepsilon}. \tag{1.7}$$

For more general (but somewhat weaker) results of this nature, where 3 is replaced by k, see [3].

If $B(kn)-B(n) < 0$ we say n is a *k-flimsy* number. We call a number *flimsy* if it is k-flimsy for some k. It seems natural to conjecture that for distinct odd integers $k_1, k_2 \geqslant 3$ the properties k_1-flimsy and k_2-flimsy are statistically independent in some reasonable sense. However, this seems to be very difficult to establish, and may be the main barrier to a proof of the zero density hypothesis for sturdy numbers.

Call an integer *k-sturdy* if it is not *k-flimsy*. The Gaussian distribution result (1.4) indicates that there are about the same number of each type of integer, so one might ask whether there is a *natural* one-to-one correspondence between the two types of integers. During an offhand discussion Professor W. M. Schmidt indicated certain partial correspondences of this kind. In Section 4 we generalize these correspondences somewhat, prove them, and use them to provide rough estimates on the distribution of k-sturdy and k-flimsy numbers.

We now review some basic properties of $B(n)$. It is clear that $B(1) = 1$ $B(2n) = B(n)$, and $B(2n+1) = B(n)+1$; indeed, the function $B(n)$ may be defined inductively by these three equalities. It is also easy to verify that $B(n+m) \leqslant B(n)+B(m)$ and $B(nm) \leqslant B(n)B(m)$. By applying the first of these to $B[(n-2^e)+2^e]$, where $n > 2^e$, we obtain

$$B(n)-1 \leqslant B(n-2^e). \tag{1.3}$$

These properties will be used throughout the paper, generally without comment.

We conclude in Section 5 with some further observations on sturdy and flimsy numbers. For a fairly comprehensive guide to the literature on $B(n)$ see [4] and also [3], [5].

2. Infinite classes of sturdy numbers. Let e, k and r denote positive integers.

THEOREM 2.1. *If $n = (2^{re}-1)/(2^e-1)$, then $B(kn) \geqslant B(n)$ for all k.*

Proof. Use induction on k. Since

$$n = 1+2^e+2^{2e}+\ldots+2^{(r-1)e},$$

the theorem is clearly true for $1 \leqslant k < 2^e$. For $k \geqslant 2^e$, write $k = 2^e s+t$ where $0 \leqslant t < 2^e$. If t is even we have that

$$B(kn) = B(kn/2) \geqslant B(n)$$

by the induction hypothesis. Hence we can assume $t = 2t'+1$ where $t' \geqslant 0$. We shall consider the cases $s = 2s'+1$ (here $s' \geqslant 0$) and $s = 2s'$ (here $s' \geqslant 1$) separately.

For s odd, the basic properties of $B(n)$ (including (1.3)) yield

$$\begin{aligned} B(kn) &= B\{(s+t)n+sn(2^e-1)\} \\ &= B\{(s+t)n+s'(2+2^2+\ldots+2^{re})+(2+2^2+\ldots+2^{re-1})\}+1 \\ &= B\{(s+t)n+s'(2+2^2+\ldots+2^{re})+ \\ &\qquad +(2+2^2+\ldots+2^{re})-2^{re}\}+1 \\ &\geqslant B\{(s+t)n+(s'+1)(2+2^2+\ldots 2^{re})\} \\ &= B\{(s'+1+t')n+(s'+1)n(2^e-1)\} \\ &= B\{[2^e(s'+1)+t']n\}. \end{aligned} \tag{2.1}$$

Since $2^e(s'+1)+t' < 2^e s+t$, the result follows by induction in this case. For s even, the same sort of reasoning gives

$$\begin{aligned} B(kn) &= B\{2(s'+t')n+(2^e+2^{2e}+\ldots+2^{(r-1)e})+ \\ &\qquad +s'(2+2^2+\ldots+2^{re})\}+1 \\ &= B\{(s'+t')n+2^{e-1}(1+2^e+\ldots+2^{(r-1)e})-2^{re-1}+ \\ &\qquad +s'(1+2+\ldots+2^{re-1})\}+1 \\ &\geqslant B\{(s'+t')n+2^{e-1}n+s'n(2^e-1)\} \\ &= B\{(2^e s'+2^{e-1}+t')n\}. \end{aligned} \tag{2.2}$$

Since $2^e s'+2^{e-1}+t' < 2^e s+t$, the result again follows by induction. This completes the proof.

We shall now obtain more information in the case $e = 1$.

LEMMA 2.1. *If $a \leqslant 2^r$ and a is even, then 2^r occurs in the binary expansion of $a(2^r-1)$. If $b \leqslant 2^{r-1}$, then 2^{r-1} occurs in the binary expansion of $b(2^r-1)$.*

Proof. The second statement, which immediately implies the first, follows from

$$b(2^r-1) \equiv 2^r-b \bmod 2^r.$$

LEMMA 2.2. *For $k \leqslant 2^r$ we have*

$$B[k(2^r-1)] = B(2^r-1) = r. \tag{2.3}$$

Proof. This is clear for $k=1$ and $k=2$. Repeat the induction step of Theorem 2.1, with $e=1$. Note that

$$(2s+t)n = 1+(2s+t+1)n-2^r.$$

In the "s odd" part of that proof there is equality throughout if 2^r occurs in the binary expansion of $(2s+1+t)n$. But $2s+1+t$ is even,

$$1 \leqslant 2s+1+t \leqslant 2^r,$$

and $n = 2^r-1$, so 2^r does occur by the previous lemma. In the "s even" part of the proof there is equality throughout if 2^{r-1} occurs in the binary expansion of $(s+1+t')n$. But since

$$1 \leqslant 2s+t \leqslant 2^r-1$$

we have

$$1 \leqslant s+1+t' \leqslant 2^{r-1}.$$

Hence we again have equality, and this completes the proof.

We comment that nothing as simple as Lemma 2.2 is valid if $k > 2^r$ or $e > 1$.

We now estimate $S(x)$. If $k \leqslant 2^r$ we have

$$B[k'k(2^r-1)] \geqslant B(2^r-1) = B[k(2^r-1)] \tag{2.4}$$

so $k(2^r-1)$ is sturdy. Choose r so that

$$2^r \leqslant \sqrt{x} < 2^{r+1}.$$

Then $k(2^r-1) \leqslant x$ for $k \leqslant 2^r$, so there are at least $2^r > .5x^{1/2}$ sturdy numbers less than or equal to x. This proves

THEOREM 2.2. $S(x) > .5x^{1/2}$.

3. The number of solutions of $B(3n)-B(n) = a$. Let $G_r(a)$ denote the number of solutions of

$$B(3n)-B(n) = a \tag{3.1}$$

for

$$2^r \leqslant n < 2^{r+1}. \tag{3.2}$$

More generally, let $G_r(a, h)$ denote the number of solutions of

$$B(3n+h)-B(n) = a \tag{3.3}$$

for n in the range described by (3.2); thus

$$G_r(a) = G_r(a, 0). \tag{3.4}$$

LEMMA 3.1. *For $h = 0$ or $h = 2$ we have*

$$G_r(a, h) = G_{r-1}(a, h/2)+G_{r-1}\big(a, (h+2)/2\big). \tag{3.5}$$

The corresponding formula for $h = 1$ is

$$G_r(a, 1) = G_{r-1}(a-1, 0)+G_{r-1}(a+1, 2). \tag{3.6}$$

Proof. Every n with $2^r \leqslant n < 2^{r+1}$ can be written uniquely as $n = 2q$ or $n = 2q+1$ with $2^{r-1} \leqslant q < 2^r$. For $h = 1$ the equation (3.3) becomes

$$B(3q)-B(q) = a-1$$

when $n = 2q$; for $n = 2q+1$ it becomes

$$B(3q+2)-B(q) = a+1.$$

The case h even is slightly simpler.

DEFINITION 3.1. Let

$$w_r(x; h) = \sum_{a=-\infty}^{\infty} G_r(a, h)x^a; \tag{3.7}$$

clearly this is a rational function of x. Note that

$$w_0(x; 0) = x, \quad w_0(x; 1) = 1, \quad w_0(x; 2) = x. \tag{3.8}$$

For any vector V, let V^{T} denote its transpose. Define

$$W_r(x) = \big(w_r(x; 0), w_r(x; 1), w_r(x; 2)\big)^{\mathrm{T}}. \tag{3.9}$$

LEMMA 3.2.

$$W_r(x) = \begin{pmatrix} 1 & 1 & 0 \\ x & 0 & x^{-1} \\ 0 & 1 & 1 \end{pmatrix}^r \begin{pmatrix} x \\ 1 \\ x \end{pmatrix}. \tag{3.10}$$

Proof. This is merely a restatement of Lemma 3.1. Since it is clear from (3.10) that

$$w_r(x; 0) = w_r(x; 2), \tag{3.11}$$

equation (3.10) is equivalent to the "contracted form"

$$\begin{pmatrix} w_r(x; 0) \\ w_r(x; 1) \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ u & 0 \end{pmatrix}^r \begin{pmatrix} x \\ 1 \end{pmatrix} \tag{3.12}$$

where $u = x+x^{-1}$.

DEFINITION 3.2. Let $p_r(u)$ be the sequence of polynomials defined by $p_{-1}(u) = 0$, $p_0(u) = 1$, and

$$p_{r+1}(u) = p_r(u)+up_{r-1}(u), \quad r \geqslant 0. \tag{3.13}$$

Set

$$q_r(x) = xp_r(x+x^{-1})+p_{r-1}(x+x^{-1}). \tag{3.14}$$

We remark that $q_r(1) = 2^r$.

LEMMA 3.3. *For $r \geqslant 0$ we have*

$$w_r(x; 0) = q_r(x) = \sum_{a=-\infty}^{\infty} G_r(a)x^a. \tag{3.15}$$

Proof. This is immediate for $r = 0$. For $r \geqslant 1$ it follows from (3.12) and

$$\begin{pmatrix} 1 & 1 \\ u & 0 \end{pmatrix}^r = \begin{pmatrix} p_r(u) & p_{r-1}(u) \\ up_{r-1}(u) & up_{r-2}(u) \end{pmatrix}. \tag{3.16}$$

Equation (3.16) is easily proved by induction.

We can now obtain an exact formula for $G_r(a)$. It is easily proved by induction that

$$p_r(u) = \sum_{i=0}^{[r/2]} \binom{r-i}{i} u^i \tag{3.17}$$

where $[x]$ denotes the greatest integer less than or equal to x. Hence

$$p_r(x+x^{-1}) = \sum_{i=0}^{r} \sum_{j=0}^{i} \binom{r-i}{i}\binom{i}{j} x^{i-2j} \tag{3.18}$$

and it follows from Lemma 3.3 that

$$G_r(a) = g_{r-1}(a) + g_r(a-1) \tag{3.19}$$

where

$$g_r(a) = \sum_{i=0}^{r}{}' \binom{r-i}{i} \binom{i}{\frac{i-a}{2}}; \tag{3.20}$$

here the dash on the summation symbol indicates that the sum is restricted to those i for which

$$i \equiv a \bmod 2. \tag{3.21}$$

Now we must estimate $g_r(a)$. Bender's paper [1] provides an excellent introduction to estimation techniques for sums of this type. We follow his approach, using the estimate

$$\binom{r}{k} = \left(\frac{2}{\pi r}\right)^{1/2} 2^r \left\{1 + O\left(\frac{1}{r-2j}\right)\right\} \exp\left[\frac{-2j^2}{r} + O(j^3 r^{-2})\right] \tag{3.22}$$

where $j = |(r/2)-k|$. The estimate (3.22) is a consequence of Stirling's formula.

Theorem. *Let* $\frac{1}{2} < s < \frac{2}{3}$. *Then*

$$g_r(a) \sim (2/3\pi r)^{1/2} 2^r \exp(-3a^2/2r), \quad |a| \leqslant r^s \tag{3.23}$$

and

$$g_r(a) = O[r2^r \exp(-r^{2s-1})], \quad |a| > r^s. \tag{3.24}$$

Proof. First assume r is a multiple of 6. Then the change of variable $i = t + r/3$ shows that

$$g_r(a) = \sum_{t=-r/3}^{r/6}{}' \binom{2r/3-t}{r/3+t} \binom{r/3+t}{r/6+t/2-a/2} \tag{3.25}$$

where the dash indicates that the sum is restricted to t such that

$$t \equiv a - r/3 \bmod 2. \tag{3.26}$$

We first consider the case $|a| > r^s$. From (3.22) we see that

$$\binom{2r/3-t}{r/3+t} = O(2^{2r/3-t}) \tag{3.27}$$

and

$$\binom{r/3+t}{r/6+t/2-a/2} = O[2^{r/3+t} \exp(-a^2/2(r/3+t))] \tag{3.28}$$

so

$$g_r(a) = O[r2^r \exp(-r^{2s-1})] \tag{3.29}$$

follows from (3.24) by the trivial estimate. Henceforth we assume that $|a| \leqslant r^s$.

We now estimate the terms for which $|t| \geqslant r^\alpha$ where $\frac{1}{2} < \alpha < \frac{2}{3}$. We have, for the individual factors,

$$\binom{2r/3-t}{r/3+t} = O[r^{-1/2} 2^{2r/3-t} \exp(-9t^2/2r)] \tag{3.30}$$

and

$$\binom{r/3+t}{r/6+t/2-a/2} = O[2^{r/3+t} \exp(-a^2/r)] \tag{3.31}$$

so the sum of the terms is

$$O[r^{1/2} 2^r \exp(-9r^{2\alpha-1}/2)]. \tag{3.32}$$

We next estimate the terms for which $|t| < r^\alpha$. Let $f(t)$ denote a typical term. Then by (3.22) we have

$$f(t) = \binom{2r/3-t}{r/3+t}\binom{r/3+t}{r/6+t/2-a/2} = K(a, r, t) \exp[O(t^3 r^{-2} + a^3 r^{-2})] \tag{3.33}$$

where

(3.34)

$$K(a, r, t) = \left[2/\pi\left(\frac{2r}{3} - t\right)^{1/2}\left(\frac{r}{3} + t\right)^{1/2}\right] 2^r \exp\left[\frac{-9t^2}{(4r/3)-2t} - \frac{a^2}{(2r/3)+2t}\right].$$

Now

$$\frac{K(a,r,t+1)}{K(a,r,t)} = 1+O(r^{-1/3}) \tag{3.35}$$

so the asymptotic behavior of the sum remains the same if we drop the congruence condition and introduce a factor of 1/2.

We now have

$$f(t) = \frac{3\sqrt{2}}{\pi r}2^r[1+O(r^{-\varepsilon})]\exp(-3a^2/2r-3^3t^2/2^2r) \tag{3.36}$$

for some $\varepsilon > 0$. Since

$$\sum_{|t|<r^\alpha} \exp(-3^3t^2/2^2r) = \int_{-\infty}^{\infty} \exp(-3^3t^2/2^2r)\,dt + O(r^{\alpha-1}) = \tfrac{2}{3}(\pi r/3)^{1/2}[1+O(r^{\alpha-3/2})] \tag{3.37}$$

we have

(3.38)
$$\frac{1}{2}\sum_{t=-r/3}^{r/6} f(t) = (2/3\pi r)^{1/2}2^r e^{-3a^2/2r}[1+O(r^{-\varepsilon})]+O[r^{1/2}2^r\exp(-9r^{2\alpha-1}/2)].$$

Now choose α so that $\frac{1}{2} < s < \alpha < \frac{2}{3}$, and recall that $|a| < r^s$; it follows that the theorem is valid when $6|r$. Now formula (3.35) shows that our approximations will not be affected if every t is replaced by $t+\theta$ where $0 \leqslant \theta \leqslant 1$, so the restriction of r to multiples of 6 is easily seen to be unnecessary. This completes the proof.

The results (1.4) and (1.6) follow immediately from (3.19) and (3.23).

4. Complementary integers. Here we establish generalizations of some facts observed by W. M. Schmidt. For integers n satisfying $1 \leqslant n \leqslant 2^{r+1}-1$ we define the complementary integer n' by

$$n+n' = 2^{r+1}-1. \tag{4.1}$$

The binary representation of n' can be obtained from that of n by replacing every 0 with 1 and every 1 with 0.

LEMMA 4.1. *Let z denote an integer. Then*

$$B(2^r-1-z)+B(2^{r-1}+z) = \begin{cases} r, & -2^{r-1} < z < 0, \\ r+1, & 0 \leqslant z < 2^{r-1}, \\ r, & 2^{r-1} \leqslant z < 2^r-1. \end{cases} \tag{4.2}$$

Proof. If $-2^{r-1} < z < 0$, write $z = t-2^{r-1}$ where $0 < t < 2^{r-1}$. Then the left side of (4.2) is

$$B(2^r+[2^{r-1}-1-t])+B(t) = 1+B(2^{r-1}-1) = r.$$

If $0 \leqslant z < 2^{r-1}$ then the left side is

$$r-B(z)+1+B(z) = r+1.$$

Finally, if $2^{r-1} \leqslant z < 2^r-1$, the left side is

$$[r-B(z)]+B(z) = r.$$

PROPOSITION 4.1. *Let $1 < n < 2^{r+1}-1$ and $4|n$. Then*

$$B(3n)+B(3n') = B(n)+B(n') = r+1 \tag{4.3}$$

unless

$$2^{r+1}/3 < n < 2^{r+2}/3; \tag{4.4}$$

if (4.4) is valid, then

$$B(3n)+B(3n') = B(n)+B(n')+1 = r+2. \tag{4.5}$$

Proof. Let $n = 4y$, and $z = 3y-2^{r-1}$. If

$$1 < n < 2^{r+1}/3$$

then $-2^{r-1} < z < 0$, so

$$B(2^r+2^{r-1}-1-3y)+B(3y) = r$$

by Lemma 4.1. Since $B(4m) = B(m)$ we deduce that

$$B[3(2^{r+1}-1)-1-12y]+B(12y) = r.$$

Next, since $B(2m)+1 = B(2m+1)$, the addition of 1 to both sides yields

$$B[3(2^{r+1}-1-4y)]+B[3(4y)] = r+1.$$

Since $n = 4y$, we have proved (4.3) for these n. The intervals

$$2^{r+1}/3 < n < 2^{r+2}/3; \quad 2^{r+2}/3 < n < 2^{r+1}-1$$

are handled in exactly the same way.

We remark that equation (4.3) can be written as

$$B(3n)-B(n) = -[B(3n')-B(n')].$$

Hence if $B(3n) \neq B(n)$ and n satisfies the hypotheses for (4.3), then n is 3-sturdy if and only if n' is 3-flimsy.

We next prove a result similar to Proposition 4.1 with a general odd integer k in place of 3.

LEMMA 4.2. *Let k and y be positive integers with k odd. Choose integers a and r so that*

$$2^a < k < 2^{a+1} \tag{4.6}$$

and $a \leqslant r$. Let

$$z = ky - u \tag{4.7}$$

where

$$u = 2^r(2^{-a}k - 1). \tag{4.8}$$

Then

$$B(2^r - 1 - z) + B(u + z) = r + B(k) - 1 - a \tag{4.9}$$

for

$$-u < z \leqslant 2^{r-a} - 1 - u. \tag{4.10}$$

Proof. Since

$$0 < ky \leqslant 2^{r-a} - 1,$$

the left side of (4.9) is

$$B[2^{r-a}(k-1) + (2^{r-a} - 1 - ky)] + B(ky)$$
$$= B[2^{r-a}(k-1) + 2^{r-a} - 1] = B(k) - 1 + r - a.$$

LEMMA 4.3. *If*

$$-u < z \leqslant 2^{r-a} - 1 - u \tag{4.11}$$

then under the hypotheses of Lemma 4.2 we have for $b > a$ that

$$B[k(2^{r+b-a} - 1 - 2^b y)] + B(k2^b y) = r + b - a. \tag{4.12}$$

Proof. From Lemma 4.2 and the fact that $B(2^b m) = B(m)$, we deduce that

$$B(k2^{r+b-a} - 2^b - k2^b y) + B(k2^b y) = r + B(k) - 1 - a. \tag{4.13}$$

Hence

$$B(p - q) + B(k2^b y) = r + B(k) - 1 - a$$

where

$$p = k(2^{r+b-a} - 1 - 2^b y) \quad \text{and} \quad q = (2^b - 1) - (k - 1).$$

Now $p > 2^b$ and $q < 2^b$; moreover, $p \equiv q \bmod 2^b$. Hence

$$B(p - q) = B(p) - B(q).$$

Since k is odd and $k < 2^{a+1} \leqslant 2^b$, we have

$$B(q) = b - B(k) + 1$$

and the result follows.

PROPOSITION 4.2. *Given a positive odd integer k, let a be the integer such that $2^a < k < 2^{a+1}$, and let $r \geqslant a$. If*

$$0 < n < (2^{r+1} - 2^{a+1})/k \tag{4.14}$$

and

$$2^{a+1} | n, \tag{4.15}$$

then

$$B(kn) + B(kn') = B(n) + B(n') = r + 1. \tag{4.16}$$

Proof. We use the notation of Lemma 4.2. Write $n = 2^{a+1}y$ and $z = ky - u$. Then

$$0 < ky < 2^{r-a} - 1,$$

so

$$-u < z < 2^{r-a} - 1 - u.$$

The result follows from Lemma 4.3 with $b = a + 1$.

We now give two applications of Proposition 4.2.

PROPOSITION 4.3. *Let $F_k(x)$ and $S_k(x)$ denote respectively the number of k-flimsy and k-sturdy integers less than or equal to x. Then for $x \to \infty$ we have*

$$\liminf F_k(x)/x \geqslant 1/2k^2, \qquad \liminf S_k(x)/x \geqslant 1/2k^2. \tag{4.17}$$

Proof. Let $E = E(r, k)$ be the number of integers for which

$$B(kn) - B(n) = 0, \qquad 1 \leqslant n \leqslant 2^{r+1}. \tag{4.18}$$

The main result of [3] immediately yields

$$E = o(2^r). \tag{4.19}$$

Next, there are at least

$$(2^{r+1}/2^{a+1}k) - 1 - E \tag{4.20}$$

integers n in the interval $[1, 2^{r+1}]$ to which Proposition 4.2 applies. If any of these fails to be k-flimsy (k-sturdy) its complement will have this property, so the result follows from (4.19), (4.20), and $2^{a+1} < 2k$.

We remark it is likely that both limits in (4.17) exist and have the constant value $1/2$ for every k.

PROPOSITION 4.4. *If k is odd, there is an $m < 8k^2$ such that m is k-flimsy.*

Proof. Take $r = 2a + 2$ and $n = 2^{a+1}$ in Proposition 4.2. Then

$$n' = 2^{2a+3} - 2^{a+1} - 1$$

and

$$2 + B(kn') \leqslant B(kn) + B(kn') = 1 + B(n').$$

Thus $B(kn') < B(n')$, so n' is k-flimsy. Since $n' < 2^{2a+3} < 8k^2$, the proof is complete.

5. Some further remarks. As with all apparently irregular sequences, one can ask a large variety of questions about the distribution of sturdy and flimsy numbers. The following facts can be shown by various elementary (and sometimes simple) arguments.

For $\varepsilon > 0$ and x sufficiently large, there is a 3-flimsy number between $x - x^{2/3+\varepsilon}$ and $x + x^{2/3+\varepsilon}$; also there is a sturdy number between $x - 3x^{1/2}$ and x. There are $\gg x^{1/5}$ consecutive 3-sturdy numbers which are $\ll x$; also $\gg x^{1/5}$ consecutive 3-flimsy numbers which are $\ll x$. Given an integer $n \geqslant 1$, there is an integer $k \leqslant 2^{n-1}B(n)/n$ such that kn is sturdy, and an integer $k \leqslant 16^{(\log 2n)^2}$ such that kn is flimsy (here the logarithm is taken to the base 2).

In response to a question of the author, the referee has remarked that standard results on prime distribution in arithmetic progressions imply that at least "half" the primes are flimsy. Simply consider the primes congruent to 3 or 5 modulo 8. They satisfy

$$2^{(p-1)/2} \equiv (2/p) \equiv -1 \bmod p.$$

Hence there are integers a and k such that the relation $kp = 1 + 2^a$ holds. The referee also points out that an argument of Hasse [2] shows that in fact more than half the primes satisfy such a relation.

References

[1] E. A. Bender, *Asymptotic methods in enumeration*, SIAM Review 16 (1974), pp. 485–515.

[2] H. Hasse, *Über die Dichte der Primzahlen p, für die eine vorgegebene ganzrationale Zahl a ≠ 0 von gerader bzw. ungerader Ordnung* mod. *p ist*, Math. Ann. 166 (1966), pp. 19–23.

[3] J. Muskat and K. B. Stolarsky, *The number of binary digits in multiplies of n*, in preparation.

[4] K. B. Stolarsky, *Power and exponential sums of digital sums related to binomial coefficient parity*, SIAM J. Applied Math. 32 (1977), pp. 717–730.

[5] — *The binary digits of a power*, Proc. Amer. Math. Soc. 71 (1978), pp. 1–5.

DEPARTMENT OF MATHEMATICS
UNIVERSITY OF ILLINOIS
Urbana, Illinois 61801

Received on 23. 9. 1977
and in revised form on 23. 3. 1978 (985)

ACTA ARITHMETICA
XXXVIII (1980)

Simple groups of square order and an interesting sequence of primes

by

MORRIS NEWMAN* (Santa Barbara, Calif.), DANIEL SHANKS (College Park, Md.) and H. C. WILLIAMS (Winnipeg, Man., Canada)

1. Introduction. If a simple group has a square order, we call it a *special group*. The sequence of integers 1, 7, 41, ... given by

$$s_{2m+1} = \frac{(1+\sqrt{2})^{2m+1} + (1-\sqrt{2})^{2m+1}}{2} \tag{1}$$

for $m = 0, 1, 2, \ldots$ we call *special numbers*. We are investigating two questions:

(A) Which finite groups are special?

(B) Which special numbers are prime?

Although Question (A) does not explicitly refer to primality, we will see that it leads us to Question (B).

A partial motivation for this investigation is the observation of R. Brauer [1] that the analysis of a simple group is facilitated if at least one prime dividing its order divides it to the first power only. Most simple groups do satisfy this Brauer condition but our special groups obviously do not.

We pursue (A) and (B) by following the closely analogous classical investigation into two much older questions:

(A_0) Which integers N are perfect?

(B_0) Which Mersenne numbers

$$M_{2m+1} = 2^{2m+1} - 1 \tag{2}$$

are prime?

As before, (A_0) does not explicitly mention primality but it leads us to (B_0) as follows:

* The work of this author was supported in part by NSF grant MCS 76-82923.