Europ. J. Combinatorics (1989) **10**, 113–135

Tight *t*-Designs and Squarefree Integers

E. Bannai and S. G. Hoggar

The authors prove, using a variety of number-theoretical methods, that tight t-designs in the projective spaces FP^n of 'lines' through the origin in F^{n+1} ($F = \mathbb{C}$, or the quarternions H) satisfy $t \leqslant 5$.

Such a design is a generalisation of a combinatorial t-design. It is known that $t \leqslant 5$ in the cases $\mathbb{F} = \mathbb{R}$, $\mathbb{O}$ (the octonions) and that $t \leqslant 11$ for tight spherical t-designs; hence the author's result essentially completes the classification of tight t-designs in compact connected symmetric spaces of rank 1.

1. Introduction

The story of t-designs goes back to the combinatorial type, generalised by Delsarte–Goethals–Seidel [7] to t-designs on a sphere, and by Neumier [22] to t-designs in a Delsarte space, including the projective spaces $\mathbb{FP}^n$ of 'lines' through the origin in $\mathbb{F}^{n+1}$, where $\mathbb{F}$ denotes the real numbers $\mathbb{R}$, complex number $\mathbb{C}$, quarternions $\mathbb{H}$, or octonions $\mathbb{O}$. (It is convenient here to use $n + 1$ for the dimension of the associated vector space, denoted by n in [3, 15]). t-designs have connections with (at least) harmonic analysis, cubature, group theory, combinatorics, and geometry. Examples and applications may be found in [5, 7, 13, 15, 17].

To state our main result, on the classification of tight t-designs, we require some notation.

Notation. Let $S = \mathbb{CP}^n$ or $\mathbb{HP}^n$. With $\mathbb{H}$ acting on $\mathbb{H}^{n+1}$ on the right, let $x = [a]$, $y = [b]$ be projective points in S with representative unit vectors a, b. The *inner product* (x, y) equals $|a^*b|^2$, where a^* denotes the conjugate transpose of a. The following applies to a finite subset $X \subseteq S$:

$$\begin{aligned}
A &= \{(x, y)\colon x, y \in X,\ x \neq y\};\\
m &= \tfrac{1}{2}(\mathbb{F}\colon \mathbb{R});\ \varepsilon = 1 \text{ if } 0 \in A, \text{ otherwise } \varepsilon = 0;\\
k &= |A \backslash \{0\}|; \qquad \sigma = mn; \qquad \tau = m + \varepsilon - 1;\\
Y &= 2k + \sigma + \tau; \qquad z = k + \tau;\\
Q_k(x) &= \frac{{}_{2k+\varepsilon}(Y)}{{}_{k+\varepsilon}(z) \cdot k!} \sum_{i=0}^{k} (-1)^i \binom{k}{i} \frac{{}_i(z)}{{}_i(Y-1)} x^{k-i};\\
R_k(x) &= Q_0(x) + Q_1(x) + \cdots + Q_k(x),
\end{aligned}$$

which equals the expression for $Q_k(x)$ but with '$Y - 1$' replaced by 'Y' [15]. Here, ${}_0(a) = 1 = (a)_0$ and ${}_r(a) = a(a - 1) \ldots (a - r + 1)$, $(a)_r = a(a + 1) \ldots (a + r - 1)$ ($r \in \mathbb{N}$).

In fact $R_k(x) = ((\sigma + m)_{k+\varepsilon}/(m)_{k+\varepsilon})P_k^{(\sigma,\tau)}(2x - 1)$, and $Q_k(x) = (Y.(\sigma + m)_{k+\varepsilon-1}/(m)_{k+\varepsilon})P_k^{(\sigma-1,\tau)}(2x - 1)$ [15], where the Jacobi polynomials $P_k^{(\sigma,\tau)}(y)$ (see [26], Chapter IV) arise in a definition of t-design via harmonic analysis on S [3].

1.2 Definition. A finite subset $X \subseteq S$ is a *t-design* in S if

$$\sum_{x \in X} Q_i((x, y)) = 0, \qquad \forall y \in X, \quad i = 1, 2, \ldots, t.$$

For the extra condition of tightness we need a background result [3], [22, pages 70–81].

0195-6698/89/020113+23 $02.00/0

1.3 Theorem. *In the notation of* 1.1, *every t-design X in S satisfies* $t \leqslant 2k + \varepsilon$ *and* $|X| \geqslant R_k(1)$.

1.4 Definition. A *tight* t-design is a t-design for which $t = 2k + \varepsilon$ or equivalently ([3, 22]), for which $|X| = R_k(1)$.

Note that $R_k(1) = (\sigma + m)_{k+\varepsilon}.(\sigma + 1)_k/(m)_{k+\varepsilon}.k!$

1.5 Theorem (main result). *If X is a tight t-design in one of the projective spaces* $\mathbb{C}\mathbb{P}^n$ *or* $\mathbb{H}\mathbb{P}^n$, *then* $t \leqslant 5$.

1.6 Remark. With [1, 2, 16] this confirms the conjecture [16] that $t \leqslant 5$ for all tight t-designs in $\mathbb{F}\mathbb{P}^n$, for each of $\mathbb{F} = \mathbb{R}, \mathbb{C}, \mathbb{H}, \mathbb{O}$. For general $\mathbb{F}$ this is best possible in the sense that tight 5-designs in $\mathbb{R}\mathbb{P}^n$ and $\mathbb{O}\mathbb{P}^n$ are known. Examples are given below. As far as the authors are aware, the existence of tight 5-designs in $\mathbb{C}\mathbb{P}^n$ and $\mathbb{H}\mathbb{P}^n$ remains in open question—to be explored elsewhere as part of an attempt to resolve the 'unknowns' in the table below.[†]

Example 1 (Example 11 of [15]). A tight 5-design of 98280 points in $\mathbb{R}\mathbb{P}^{23}$ with $A = \{0, \frac{1}{16}, \frac{1}{4}\}$ is obtained from the minimal vectors of the Leech lattice.

Example 2 (Example 10 of [15]). There is a tight 5-design of 819 points in the Cayley plane $\mathbb{O}\mathbb{P}^2$, related to group ${}^3D_4(2)$, and forming a generalised hexagon based on $A = \{0, \frac{1}{4}, \frac{1}{2}\}$ (see [6] for full details).

It is known [2] that $t \leqslant 11$ for tight t-designs on a *sphere* in $\mathbb{R}^{n+1}$ ($n \geqslant 1$). Indeed, for $n \geqslant 2$ they exist precisely for $t = 2, 3, 4, 5, 7, 11$. Examples are found in 8·3 to 8·5 of [7], which yield also the tight t-designs in $\mathbb{R}\mathbb{P}^n$ that are cited in the following table along with examples 2 to 10 of [15]:

Some tight t-designs in $\mathbb{F}\mathbb{P}^n$ ($\mathbb{F} = \mathbb{R}, \mathbb{C}, \mathbb{H}, \mathbb{O}$)

	$\mathbb{R}P^n$	$\mathbb{C}P^n$	$\mathbb{H}P^n$	$\mathbb{O}P^n$
$t = 2$	8·3	5, 8	Unknown	Unknown
$t = 3$	8·4	2, 6, 7	3, 9	4
$t = 4$	none	Unknown	Unknown	Unknown
$t = 5$	8·5	Unknown	Unknown	10

Spheres, together with the $\mathbb{F}\mathbb{P}^n$ above, constitute the spaces in the following corollary.

1.7 Corollary. *If X is a tight t-design in one of the compact connected symmetric spaces of rank* 1 *and topological dimension greater than* 1, *then*
(*a*) $t \leqslant 11$,
(*b*) *for any pair of distinct points, the associated inner product is the reciprocal of an integer.*

Proof. For (a) the preceding remarks suffice. Part (b) is known in the spherical case and for $\mathbb{F}\mathbb{P}^n$ with $\mathbb{F} = \mathbb{R}, \mathbb{O}$ [1, 2, 16]. For $\mathbb{F} = \mathbb{C}, \mathbb{H}$ the main result, Theorem 1.5, enables us to assume $t \leqslant 5$. By Theorem 1.9 and Remark 1.12 it remains to check for four quadratic

[†] *Added in proof.* A subsequent result: the only tight 4 or 5-designs in *any* $\mathbb{F}\mathbb{P}^{d-1}$ are Examples 1 and 2 on this page. See S. G. Hoggar, Tight 4 and 5-designs in projective spaces. To appear in *Graphs and Combinatorics.*

polynomials (cases 1 to 4 of 1.8) that if the roots are rational then they are integral. This is an easy divisibility argument.

How the Main Result is Proved

1.8 Four Cases. In the notation of 1.1, we have $m = 1$ or 2 and $\varepsilon = 0$ or 1. It proves useful to consider separately the four cases of the pair (m, ε), as in the table below:

Case	m	ε	σ	τ	Y	z
1	2	0	$2n$	1	$2n + 2k + 1$	$k + 1$
2	1	1	n	1	$n + 2k + 1$	$k + 1$
3	1	0	n	0	$n + 2k$	k
4	2	1	$2n$	2	$2n + 2k + 2$	$k + 2$

1.9 Theorem [16], [22, p. 70–81]. *For a tight t-design X in S we have, in the notation of* 1.1:

(a) *the elements of A are the roots of* $x^{\varepsilon} R_k(x)$;

(b) *these roots are rational.*

The key to the proof of the main result is to show that $R_k(x)$ has at least one irrational root if $t \geqslant 6$. Our two main tools for this are Newton polygons, and the discriminant of $R_k(x)$.

1.10 The Newton Polygon [8]. Let $f(x) = \Sigma_{i=0}^{k} C_i x^i$ be an integral polynomial ($C_i \in \mathbb{Z}$). Then the *Newton polygon of* $f(x)$ *for prime p* is the lower boundary of the convex hull of $\{(i, [[C_i]]_p)\colon C_i \neq 0\}$, where $[[C_i]]_p$ denotes the index of p in C_i (see 2.1).

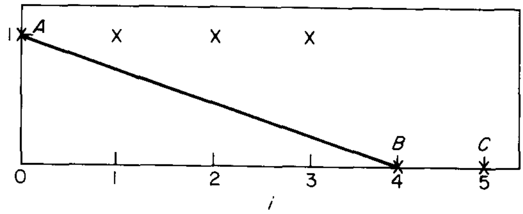
1.11 Theorem [8]. *If an edge of the Newton polygon of* $f(x)$ *for some prime has non-integral slope, then* $f(x)$ *has an irrational root.*

1.12 Remark. If C is a non-zero constant, then the roots of $f(x) = C(-x)^k R_k(-1/x)$ are the negative reciprocals of those of $R_k(x)$. In particular, $R_k(x)$ has an irrational root if and only if $f(x)$ does, and by choosing $C = k!/(m - 1)!(\sigma + m)_{k-m+1}$, we obtain an *integral* polynomial

$$f(x) = \sum_{i=0}^{k} \binom{k}{i} \binom{Y - i}{z - i} x^i. \tag{1.1}$$

Again, for the notation see 1.1.

Example 3. We evaluate $f(x)$ corresponding to a tight 11-design in $\mathbb{HP}^7$. Here $m = 2$, $\varepsilon = 1$, $k = 5$, $n = 7$, so that $Y = 26$, $z = 7$. The reader may wish to verify that the Newton polygon of $f(x)$ for prime $p = 23$ is the figure ABC below:



Since AB has non-integral slope $-\frac{1}{4}$, it follows from Theorem 1.11 that $f(x)$, hence $R_k(x)$, has an irrational root. Therefore, by Theorem 1.9, there does not exist a tight 11-design in $\mathbb{HP}^7$.

1.13 The Discriminant. Let $R_k(x)$ have roots $x_1, x_2, \ldots, x_k$. Then the *discriminant* of $R_k(x)$ is defined to be

$$\Delta = \Pi(x_i - x_j)^2 \qquad (1 \leqslant i < j \leqslant k).$$

In fact, since $R_k(x)$ is a constant multiple of the Jacobi polynomial $p_k^{(\sigma,\tau)}(2x - 1)$, we have from the results of Hilbert [26, p. 142] that

$$\Delta = \prod_{\nu=1}^{k} \nu^{\nu}(\sigma + \nu)^{\nu-1}(\tau + \nu)^{\nu-1}(\sigma + \tau + k + \nu)^{k-\nu} \tag{1.2}$$

up to multiplication by the square of a rational number. For each of Cases 1–4 we use this formula with the table of 1.8 to write down a product D, which must be the square of an *integer* if $R_k(x)$ has only rational roots.

We then prove that D *cannot* be a square by considering certain sets of squarefree integers $a_1, \ldots, a_L$ defined by $N + r_i = a_i x_i^2$ $(1 \leqslant i \leqslant L)$, where $0 < r_1 < r_2 < \cdots < r_L$, and N and the x_i are positive integers.

In Section 2 we establish inequalities for the products of such a_i, which are applied in Sections 3, 4 and 5 to obtain the desired contradiction for Cases 1, 2, 3 and 4 respectively. Newton polygons appear in Section 5; as also in Section 6, where remaining exceptional cases of k are settled by congruence techniques.

1.14 Henceforth we assume $n \geqslant k^2$. The case $1 < n < k^2$ was settled in [4], partly on the basis of the following theorem, which we prove in Section 7.

1.15 Theorem. *Let M, r be positive integers satisfying $r \geqslant 63$, $M \geqslant 2r$. Then $(M)_r$ has a prime divisor $p > 2r$.*

2. Prime Numbers and Squarefree Integers

The results of this section are crucial for exploiting the fact that if $R_k(x)$ has no irrational root then its discriminant is a square.

2.1 Notation. Let N, L, $N_1, \ldots, N_L$ be positive integers, p a prime.

$[N_1 N_2 \ldots N_L]_p$ = (number of factors N_i divisible by p).

$[[N]]_p$ = p-index I of N, the highest power of p that divides N. We also write $p^I \parallel N$.

$[N]$ = greatest integer not exceeding N.

$\langle N \rangle$ = $N - [N]$, the fractional part of N.

$\lceil N \rceil$ = least integer not less than N.

Examples. $[N!]_p$ will be taken to mean $[1, 2 \ldots N]_p$, which equals $[N/p]$.

$$[[N!]]_p = \sum_{i=1}^{\infty} [N/p^i]; \tag{2.1}$$

$$\left.\begin{aligned} [x] + [y] \leqslant [x + y] \leqslant [x] + [y] + 1 \\ [x - y] \leqslant [x] - [y] \leqslant [x - y] + 1 \end{aligned}\right\}; \tag{2.2}$$

$$1 + \left[\frac{N - 1}{p}\right] = \left\lceil \frac{N}{p} \right\rceil \qquad (p, N \in \mathbb{N}). \tag{2.3}$$

2.2A LEMMA. *Let p be any prime. Let the integer $L > 1$ have p-adic expansion $d_0 + d_1 p + \cdots + d_r p^r$, with digit sum $d = \Sigma\, d_i$. Then*

(i) $\sum_{j=1}^{\infty} \left\langle \frac{L}{p^j} \right\rangle = \frac{d}{p-1}$;

(ii) $\sum_{j=1}^{\infty} (-1)^{j+1} \left\langle \frac{L}{p^j} \right\rangle = (d_0 - d_1 + d_2 - \ldots)/(p+1)$;

(iii) *if* $p^\alpha \| L!$ *then* $\alpha = (L-d)/(p-1)$.

PROOF. (i)

$$\sum_{j=1}^{\infty} \left\langle \frac{L}{p^j} \right\rangle = \sum_{j=1}^{\infty} \left\langle \sum_{i=0}^{r} d_i p^{i-j} \right\rangle$$

$$= \sum_{i=0}^{r} \sum_{j=i+1}^{\infty} d_i p^{i-j} = \sum_{i=0}^{r} d_i \sum_{s=1}^{\infty} \frac{1}{p^s} = \frac{d}{p-1}.$$

(ii) This is a similar calculation to (i), taking account of the factor $(-1)^{j+1} = (-1)^i(-1)^{s+1}$, $s = j - i$.

(iii) This is an old result of Legendre which we need, conveniently reproved here for completeness. We have, using (2.1),

$$\alpha = \sum_{i=1}^{\infty} \left[\frac{L}{p^i} \right] = \sum_{i=1}^{\infty} \frac{L}{p^i} - \sum_{i=1}^{\infty} \left\langle \frac{L}{p^i} \right\rangle$$

$$= \frac{L}{p-1} - \frac{d}{p-1}, \text{ by part (i).}$$

2.2 THEOREM. *For any prime p, and integer $L > 1$, let $p^\alpha \| L!$. Then*

$$\alpha \geqslant \frac{L}{p-1} - \log_p (L+1).$$

PROOF. Let L have p-adic expansion $d_0 + d_1 p + \cdots + d_r p^r$, with digit sum $\Sigma\, d_i = d = t(p-1) + u$, where $t \in \mathbb{Z}$, $0 \leqslant u < p - 1$. The least positive integer with digit sum d is

$$L_0 = (p-1) + (p-1)p + \cdots + (p-1)p^{t-1} + up^t.$$

Then $L_0 \leqslant L$, and (from the fact that $f(x) = x^{1/(x-1)}$ is decreasing for $x \geqslant 3$) we have $p^u \leqslant (u+1)^{p-1}$ $(0 \leqslant u < p-1)$, and so

$$\log_p(L_0 + 1) = \log_p((u+1)p^t) = \log_p(u+1) + t \geqslant \frac{u}{p-1} + t.$$

So we obtain

$$\alpha = \frac{L}{p-1} - \frac{d}{p-1}, \quad \text{by Lemma 2.2A(iii),}$$

$$= \frac{L}{p-1} - t - \frac{u}{p-1}, \quad \text{on substituting for } d,$$

$$\geqslant \frac{L}{p-1} - \log_p(L_0 + 1)$$

$$\geqslant \frac{L}{p-1} - \log_p (L+1).$$

(Equality occurs if and only if $L + 1$ is a power of p.)

2.3 THEOREM. *Let p be a prime. For positive integers L, $M (L > 1)$ write $M + i = a_i x_i^2$, $1 \leqslant i \leqslant L$, where the a_i are squarefree integers. Then*:

(a) $[a_1 \ldots a_L]_p \leqslant 1 + [(L-1)!]_p \, (= \lceil L/p \rceil)$;

(b) $[a_1 \ldots a_L]_p \leqslant \dfrac{L+1}{p+1} + \dfrac{p-1}{p+1} \log_p \left(\dfrac{p+1}{2} L + \dfrac{p-1}{2} \right)$;

(c) *if $M \geqslant L^2/4$ then the a_i are distinct.*

PROOF. (a) Let $M + R + 1$ be a factor amongst $M + 1, \ldots, M + L$ with highest p-index. Then $[M + i]_p = [(M + R + 1) - (M + i)]_p = [R + 1 - i]_p$, and so $[a_1 \ldots a_L]_p \leqslant [R!]_p$. Indeed, writing $S = L - R - 1$, we have

$$\begin{aligned}[a_1 \ldots a_L]_p &\leqslant 1 + [a_1 \ldots a_R]_p + [a_{R+z} \ldots a_L]_p \\ &\leqslant 1 + [R/p] + [S/p] \\ &\leqslant 1 + \left\lceil \frac{R+S}{p} \right\rceil,\end{aligned}$$

by (2.2), which equals the right-hand side of (a).

(b) We use a refinement of the above argument, employing the fact that factors $M + i$ with even p-index do not contribute to $[a_1 \ldots a_L]_p$. We have

$$\begin{aligned}[a_1 \ldots a_L]_p &\leqslant 1 + \sum_{i=1}^{\infty} (-1)^{i+1} [R/p^i] + \sum_{i=1}^{\infty} (-1)^{i+1} [S/p^i] \\ &= 1 + \sum_{i=1}^{\infty} (-1)^{i+1} \left(\frac{R}{p^i} - \left\langle \frac{R}{p^i} \right\rangle + \frac{S}{p^i} - \left\langle \frac{S}{p^i} \right\rangle \right) \\ &= 1 + \frac{R+S}{p+1} - \sum_{i=1}^{\infty} (-1)^{i+1} \left(\left\langle \frac{R}{p^i} \right\rangle + \left\langle \frac{S}{p^i} \right\rangle \right).\end{aligned}$$

Let R, S have respective p-adic expansions $\Sigma_{i=0}^{r} b_i p^i$ and $\Sigma_{i=0}^{s} c_i p^i$. Then by 2.2A(ii) the above expression yields

$$[a_1 \ldots a_L]_p \leqslant (L + p + e)/(p + 1) \tag{2.4}$$

where (as before) $R + S = L - 1$, and $e = -b_0 - c_0 + b_1 + c_1 - b_2 - c_2 + \ldots$. Without loss of generality we may assume $e > 0$, and write $e = 2t(p-1) + u$ for integers t, u with $0 \leqslant u < 2(p-1)$. The smallest integer L_0 which is the sum of two integers $\Sigma \, b_i' p^i$ and $\Sigma \, c_i' p^i$ such that $-b_0' - c_0' + b_1' + c_1' - \ldots = e$ is $L_0 = 2(p-1)p + 2(p-1)p^3 + 2(p-1)p^5 + \cdots + 2(p-1)p^{2t-1} + up^{2t+1}$. Thus

$$L - 1 \geqslant L_0 = u . p^{2t+1} + 2(p-1)p(1 - p^{2t})/(1 - p^2),$$

whence

$$(p + 1)L \geqslant (u(p + 1) + 2)p^{2t+1} - (p - 1),$$

so that

$$\log_p(L(p + 1) + (p - 1)) \geqslant 2t + 1 + \log_p(u(p + 1) + 2). \tag{2.5}$$

Substituting for e in (2.4) and using (2.5) to give an upper bound for t, we obtain

$$\begin{aligned}&[a_1 \ldots a_L]_p \leqslant (L + p + 2t(p-1) + u)/(p + 1) \\ &\leqslant \frac{L+1}{p+1} + \frac{p-1}{p+1} (\log_p(L(p + 1) + p - 1) - \log_p(u(p + 1) + 2)) + \frac{u}{p+1}.\end{aligned}$$

To complete the proof it suffices to show that $u \leqslant (p-1)\log_p(\frac{1}{2}u(p+1)+1)$, or equivalently

$$p^{u/(p-1)} \leqslant \tfrac{1}{2}u(p+1)+1,$$

for $0 \leqslant u < 2p-2$. But this follows from the fact that both sides are equal for $u = 0$, $u = 2p-2$, and that the second derivative of the left-hand side is positive while that of the right-hand side vanishes.

(c) We slightly sharpen a calculation of Erdös in [10]. Suppose $M + i = ax_i^2$, $M + j = ax_j^2$, with $1 \leqslant i < j \leqslant L$. Then $L - 1 \geqslant |(M+j)-(M+i)| = a(x_j^2 - x_i^2) \geqslant \sqrt{a}(x_j + x_i) < 2\sqrt{M}$.

2.4 Theorem. *For positive integers L, N write* $N + 2i = A_iX_i^2$, $1 \leqslant i \leqslant L$, *where the* A_i *are squarefree. Then, for odd primes p*:

(a) $[A_1 \ldots A_L]_p \leqslant 1 + [(L-1)!]_p (=\lceil L/p \rceil)$:

(b) $[A_1 \ldots A_L]_p \leqslant \dfrac{L+1}{p+1} + \dfrac{p-1}{p+1}\log_p\left(\dfrac{p+1}{2}L + \dfrac{p-1}{2}\right)$;

and for $p = 2$,

(c) $[A_1 \ldots A_L]_2 \leqslant \dfrac{2L}{3} + 1 + \frac{1}{3}\log_2 L$.

Proof. (a), (b). For odd prime p's the estimates for $[A_1 \ldots A_L]_p$ are exactly the same as for $[a_1 \ldots a_L]_p$ in the proof of Theorem 2.3.

(c) Put $M = N + 1$ and define $a_1, \ldots, a_{2L}$ as in 2.3. Then by 2.3(b),

$$[A_1 \ldots A_L]_2 = [a_1 \ldots a_{2L}]_2 \leqslant \frac{2L+1}{3} + \tfrac{1}{3}\log_2(3L + \tfrac{1}{2}) \leqslant \frac{2L}{3} + \tfrac{1}{3}\log_2 L + 1,$$

since $3L + \frac{1}{2} \leqslant 4L$.

We conclude with a key inequality.

2.5 Theorem [12]. *Let* $A_1, \ldots, A_L$ *be distinct squarefree integers. Then*

$$(\tfrac{3}{2})^L L! < A_1A_2 \ldots A_L \qquad (L \geqslant 64).$$

Note that we will often abbreviate the product $a_1 \ldots a_{2q}$ to Πa_i, and similarly for the A_i.

3. Case 1: $2k$-Designs in $\mathbb{HP}^n$

We are assuming $n \geqslant k^2$ and that $R_k(x)$ has only rational roots. We then find that $k \geqslant 3$ involves a contradiction. Using the table of 1.8 and formula (1.2) for the discriminant of $R_k(x)$ we find a product D which must be the square of an integer, namely

$$D = \begin{cases} (k+1)(n+1)_k & \text{if } k = 2q, \\ (n+1)_q(n+q+2)_q & \text{if } k = 2q+1. \end{cases} \tag{3.1}$$

We deal with both cases together by writing

$$\begin{aligned} n + i &= a_ix_i^2 && \text{for } 1 \leqslant i \leqslant q, \\ n + j &= a_jx_j^2 \quad \text{if } k = 2q && \left.\right\} \text{for } q+1 \leqslant j \leqslant 2q, \\ n + j + 1 &= a_jx_j^2 \quad \text{if } k = 2q+1 && \end{aligned}$$

where the a's are squarefree.

3.1 The Product $\Pi a_i : k \geqslant 143$. The technique in this range of k is to find an upper bound of Πa_i which is exceeded by the lower bound given in Theorem 2.5. The following theorem is the first step.

3.2. Theorem. For Case 1 we have

$$a_1 \dots a_{2q} \mid (2q+1)! \prod_{p<2q} p \qquad (k \geqslant 3).$$

Proof. (a) $k = 2q$, $q \geqslant 2$. Suppose $p \mid \Pi a_i$, for a prime p. Then $p \mid D$. Suppose that $p > k + 1$. Then p divides a unique $n + i$ and so, as D is a square, p has even (positive) index in this $n + i$. But this implies the contradiction $p + a_i$. Thus $p \leqslant k + 1$ must hold. If $p = k + 1$ then again p divides a unique $n + i$, but this time the factor $k + 1$ in D requires that p have odd index in $n + i$. Hence $p \parallel \Pi a_i$. $p = k(=2q)$ is impossible. For $p < k$ we use 2.3(a) to obtain $[a_1 \dots a_{2q}]_p \leqslant [(2q-1)!]_p + 1$. Thus Πa_i divides $(2q-1)!(k+1)\Pi_{p<k} p$, which in turn divides $(2q+1)!\, \Pi_{p<2q}\, p$.

(b) $k = 2q + 1$, $q \geqslant 1$. Let $p \mid \Pi a_i$ for some prime p. Then $p \mid (n+1)_k$. Case $p \geqslant k$ cannot occur, since such a p divides a unique $n + i$, so divides no a_i as D is a square. For $p < k$ we observe that our $2q$ squarefree integers a_i belong to a set of $k = 2q + 1$ such numbers corresponding to the factors of $(n+1)_k$. Hence, setting $L = 2q + 1$ in 2.3(a), we see that Πa_i divides $(2q)!\, \Pi_{p<2q+1}\, p$ which, since $2q$ is not prime, divides $(2q+1)!\, \Pi_{p<2q}\, p$. This completes the proof of Theorem 3.2.

Refining the Bound. Let $2^\alpha, 3^\beta \parallel (2q+1)!$ and $2^\gamma, 3^\delta \parallel \Pi a_i$. Then, from Theorem 3.2,

$$a_1 \dots a_{2q} \mid 2^{\gamma-\alpha} 3^{\delta-\beta} (2q+1)! \prod_{p<2q} p. \tag{3.3}$$

Setting $L = 2q + 1$ in 2.2 gives

$$\begin{aligned} \alpha &= [(2q+1)!]_2 \geqslant 2q - \log_2(q+1), \\ \beta &= [(2q+1)!]_3 \geqslant q + \tfrac{1}{2} - \log_3(2q+2). \end{aligned} \tag{3.4}$$

With $L = 2q + 1$ in 2.3(b) we obtain

$$\begin{aligned} \gamma &\leqslant \tfrac{1}{3}(2q + 2 + \log_2(3q+2)), \\ \delta &\leqslant \tfrac{1}{2}(q + 1 + \log_3(4q+3)). \end{aligned} \tag{3.5}$$

Furthermore, we have from [25, Theorems 9 and 18] the inequalities

$$\prod_{p<L} p < \begin{cases} 3^L, & L > 0, \qquad (3.6a) \\ e^L, & 0 < L < 10^8. \qquad (3.6b) \end{cases}$$

Now, by 2.3(c) with $L = k$, $M = n$, all of $a_1, \dots, a_{2q}$ are distinct, so by Theorem 2.5

$$(2q)!\, 3^{2q} 2^{-2q} < a_1 \dots a_{2q} \qquad (q \geqslant 32),$$

which, by (3.3) to (3.6a), is less than

$$2^{-4q/3} 2^{5/3} 3^{-q/2} (3q+2)^{1/3} (4q+3)^{1/2} (q+1)^2 \cdot (2q+1)!\, 3^{2q}.$$

It follows easily that

$$(\tfrac{27}{16})^{q/6} < 19(q+1)^4 \qquad (q \geqslant 32), \tag{3.7}$$

which is a contradiction for $q \geqslant 300$. On the other hand, invoking (3.6b), we have

$$\left(\frac{3}{e}\right)^{2q}\left(\frac{27}{16}\right)^{q/6} < 19(q+1)^4, \qquad 0 < q < 10^8.$$

This inequality in false for $q \geqslant 71$ ($k \geqslant 143$).

3.3. The Number of Distinct a_i: $10 \leqslant k \leqslant 142$

Case $k = 2q$, $k + 1$ *not prime*. In this case $D = (k+1)(n+1)_k$ is assumed to be a square. From Erdös and Selfridge [12] we have

If $n > k \geqslant 3$ then some prime

$p_0 \geqslant k$ has odd index in $(n+1)_k$.

But here k, $k+1$ are not prime, hence $p_0 > k+1$, and so D cannot be a square

Case $k = 2q + 1$, or $k = 2q$ with $k + 1$ *prime*. By considering the product D of (3.1), which must be a square, we have for any prime p,

$$\left.\begin{array}{l}\text{if } p < k \text{ then } p \text{ has even index in } \Pi a_i,\\ \text{if } p \geqslant k (p \neq k+1) \text{ then } p \not| \, \Pi a_i,\\ \text{if } p = k+1 \text{ then } p \,\|\, \Pi a_i.\end{array}\right\} \tag{3.8}$$

With the following lemma, this gives an effective bound on the number of a_i, yielding a contradiction.

3.4 Lemma. *If the prime p has even index in* $a_1 \ldots a_{2q}$ *then*

$$[a_1 \ldots a_{2q}]_p \leqslant \lceil k/p \rceil - (\lceil k/p \rceil \bmod 2).$$

Proof. In both cases $k = 2q$, $k = 2q + 1$ of D the q_i are a subset of the squarefree parts of k successive integers, so by 2.3(a), $[a_1 \ldots a_{2q}]_p \leqslant \lceil k/p \rceil$. But since the left-hand side is even, the bound may be reduced by 1 if $\lceil k/p \rceil$ is odd. This gives the conclusion of the lemma.

Now let p_r denote the rth prime. Since there are $2q$ integers a_i, we have

$$\begin{aligned}2q = {} & |\{i,\ 1 \leqslant i \leqslant 2q\colon \text{every prime divisor of } a_i \text{ is less than } p_r\}| \\ & + |\{i,\ 1 \leqslant i \leqslant 2q;\ a_i \text{ has a prime divisor } p \geqslant p_r\}|.\end{aligned} \tag{3.9}$$

An upper bound for the first expression in brackets is 2^{r-1}, and one for the second is, by (3.8) and Lemma 3.4,

$$Bp_r = P + \sum_{p_r \leqslant p < k} (\lceil k/p \rceil - (\lceil k/p \rceil \bmod 2)), \tag{3.10}$$

where $P = 1$ if $k + 1$ is prime; otherwise $P = 0$. Thus

$$2q \leqslant 2^{r-1} + Bp_r. \tag{3.11}$$

We obtain the following contradiction of (3.11)

$$\left.\begin{array}{ll}2q > 4 + B_5\cdot & \text{for } 10 \leqslant k \leqslant 55,\\ 2q > 8 + B_7 & \text{for } 56 \leqslant k \leqslant 142.\end{array}\right. \tag{3.12}$$

Examples:

k	10	11	55	k	55	100	142
$4 + B_5$	9	8	52	$8 + B_7$	46	93	134

3.5 Exceptional Values: $k = 3, 4, 5, 6, 7, 9$. These are dealt with in Section 6.

4. Case 2: $(2k + 1)$-Designs in $\mathbb{CP}^n$

We recall our assumption that $n \geqslant k^2$ and that $R_k(x)$ has only rational roots. Our product D which must be a square is:

$$D = \begin{cases} (K + 1)(n + 2)(n + 4) \dots (n + 4q), & \text{if } k = 2q, \\ \left.\begin{array}{l}(n + 2)(n + 4) \dots (n + 2q) \times \\ (n + 2q + 4)(n + 2q + 6) \dots (n + 4q + 2)\end{array}\right\} & \text{if } k = 2q + 1. \end{cases} \tag{4.1}$$

We then write

$$\begin{array}{lll} n + 2i = A_iX_i^2 & & \text{for } 1 \leqslant i \leqslant q, \\ n + 2j = A_jX_j^2 & \text{if } k = 2q & \multirow{2}{*}{} \\ n + 2 + 2j = A_jX_j^2 & \text{if } k = 2q + 1 & \text{for } q + 1 \leqslant j \leqslant 2q, \end{array} \tag{4.2}$$

where the A's are squarefree.

4.1 The Product ΠA_i, $k \geqslant 65$. To achieve the required upper bound for $A_1 \dots A_{2q}$ we have:

4.2 Theorem. *In Case 2,*

$$A_1 \dots A_{2q} \mid (2q + 1)! \, . \prod_{p < 2q} p \, . \, 2^\lambda \ (\textit{some } \lambda \in \mathbb{N}).$$

Proof. The argument is entirely analogous to that of Theorem 3.2 in Case 1, with 2.4(a) in place of 2.3(a). The extra factor 2^λ results from the exceptional case $p = 2$.

Refining the Bound. As before, we write $2^\alpha, 3^\beta \,\|\, (2q + 1)!$, $2^\gamma, 3^\delta \,\|\, \Pi A_i$, so that

$$A_1 \dots A_{2q} \mid 2^{\gamma - \alpha} 3^{\delta - \beta} (2q + 1)! \prod_{p < 2q} p. \tag{4.3}$$

We observe that if n is even, the problem reduces to Case 1 on taking out the square 2^{2q} from D (now $M = n/2$, $L = k$ in 2.3(c). So let us assume that n is odd. Then $\gamma = 0$ and we may set $L = 2q + 1$ in both 2.2 and 2.4(b) to obtain

$$\begin{aligned} a &\geqslant 2q - \log_2 (q + 1), \\ \beta &\leqslant q + \tfrac{1}{2} - \log_3 (2q + 2), \\ \delta &\leqslant \tfrac{1}{2}(q + 1 + \log_3(4q + 3)). \end{aligned} \tag{4.4}$$

By 2.3(c) ($L = 2k$, $M = n$) the A_i are distinct, so finally, for $q \geqslant 32$ ($2q! \, 3^{2q} 2^{-2q} <$ $A_1 \dots A_{2q}$, by Theorem 2.5, $< 2^{-2q} 3^{-q/2} . 2(q + 1)^2 (4q + 3)^{1/2} (2q + 1)! \, 3^{2q}$ by (4.3), (4.4) and (3.6a), whence

$$3^q < 64(q + 1)^7 \qquad (q \geqslant 32). \tag{4.5}$$

This is a contradiction for $q \geqslant 32$ ($k \geqslant 65$).

4.3 The Number of A_i: $3 \leqslant k \leqslant 64$. As noted earlier, we may assume that n is odd, so that 2 is a divisor of no A_i. Therefore, by the argument used for (3.11), we have an inequality of the form

$$2q \leqslant 2^{r-2} + Bp_r \qquad (r \geqslant 2) \tag{4.6}$$

where $Bp_r \geqslant |\{i,\ 1 \leqslant i \leqslant 2q\colon A_i \text{ has a prime divisor } p \geqslant p_r\}|$.

It remains to determine a suitable Bp_r for $k = 2q, 2q + 1$.

$k = 2q, k + 1$ prime. If $k + 1$ is prime, the restrictions (3.8) hold for p. As a result, the method of Case 1 rules out $10 \leqslant k \leqslant 64$ ($k + 1$ prime) with Bp_r as in (3.10). Further, using the restriction $p \neq 2$, we obtain the contradiction $2 + B_3 = 3, 5$ for $k = 4, 6$ respectively in (4.6).

$k = 2q, k + 1$ not prime. Here $p \nmid \Pi A_i$ if $p = 2$ or $p \geqslant k$, so (4.6) holds with

$$Bp_r = \sum_{p_r \leqslant p < k} \lceil k/p \rceil. \tag{4.7}$$

This gives the contradiction $4 + B_7 < 2q$ for $8 \leqslant k \leqslant 64$.

$k = 2q + 1$. Here we may again use the value of Bp_r in (3.10) with (4.6). Now Case 1 rules out the odd values $k = 11, 13, \ldots, 63$. Furthermore, (4.6) is contradicted by $1 + B_3 = 1, 3$ for $k = 3, 5$ and $2 + B_5 = 4, 6$ for $k = 7, 9$. This completes Case 2 for all $k \geqslant 3$.

5. Cases 3 and 4: $2k$-Designs in $\mathbb{CP}^n$ and $(2k + 1)$-Designs in $\mathbb{HP}^n$

We continue to assume that $n \geqslant k^2$ and that $R_k(x)$ has only rational roots. Then the following expression D is a square:

$$\begin{aligned} D &= g(q)\,.\,(N + 2)(N + 4) \ldots (N + 2q), \\ &\quad \times (Y - 1)(Y - 3) \ldots (Y - 2q + 1), \end{aligned} \tag{5.1}$$

where the values of $g(q)$, N, Y (and z for later) are given in table (5.1A) below. Henceforth 3_{2q} refers to Case 3 with $k = 2q$, and so on:

Case	N	Y	z	$g(q)$
3_{2q}	n	$n + 2k$	$2q$	$(2q)!$
3_{2q+1}	n	$n + 2k$	$2q + 1$	$(2q + 1)!$
4_{2q}	$2n$	$2n + 2k + 2$	$2q + 2$	$(2q)!(q + 1)$
4_{2q+1}	$2n$	$2n + 2k + 2$	$2q + 3$	$(2q + 1)!(q + 1)$

(5.1A)

We will again have $2q$ squarefree integers, but this time we must consider them as two sets of q. Note htat N and $Y - 1$ have opposite parity. Additional techniques to those used in Cases 1 and 2 are required. We define

$$\begin{aligned} N + 2i &= a_i x_i^2 \quad (1 \leqslant i \leqslant q); \qquad Y + 1 - 2j = b_j y_j^2 \quad (1 \leqslant j \leqslant q); \\ A &= [a_1 \ldots a_q]_p; \qquad B = [b_1 \ldots b_q]_p. \end{aligned} \tag{5.2}$$

5.1 THE PRODUCT $\Pi a_i b_j$; $k \geqslant 171$. The following theorem compares with 3.2 and 4.2:

5.2 THEOREM. *In Cases* 3 *and* 4 *we have*

$$\Pi a_i b_j \mid (2q + 3)!(2q + 1)(2q + 3). \prod_{\sqrt{2q}<p<q} p^2 . 2^l \qquad (l \in \mathbb{N}).$$

5.3 LEMMA. *Let p be an odd prime; then*
(a) $A + B \equiv [[g(q)]]_p$ (mod 2), *and*
(b) $A + B \leqslant [(2q)!]_p + 2$.

PROOF OF LEMMA 5.3. (a) holds because D is a square. For (b) we have

$$\begin{aligned} A + B &\leqslant 2([(q - 1)!]_p + 1) && \text{by 2.4(a),} \\ &\leqslant [(2q)!]_p + 2 && \text{by (2.2).} \end{aligned}$$

PROOF OF THEOREM 5.2 Since A, $B \leqslant 1$ if $p = 2q + 1$, or $p = 2q + 3$, it suffices to show that, for p an odd prime, we have

$$\begin{array}{ll} A + B \leqslant [[g(q)]]_p + 2 & \text{for all } p, \\ A + B \leqslant [[g(q)]]_p & \text{unless } \sqrt{2q} < p < q, p = 2q + 1, \text{ or } p = 2q + 3, \\ A + B = 0 & \text{if } p > 2q + 3. \end{array}$$

The first statement is immediate from 5.3(b) and the table of (5.1). For the rest, we consider three cases.

$p \leqslant \sqrt{2q}$. We have

$$\begin{aligned} A + B &\leqslant [(2q)!]_p + 2, && \text{by 5.3(b);} \\ &\leqslant [g(q)]_p + 2, && \text{from (5.1A);} \\ &\leqslant [[g(q)]]_p + 1, && \text{since } p^2 \leqslant 2q; \\ &\leqslant [[g(q)]]_p, && \text{by 5.3(a).} \end{aligned}$$

$q \leqslant p \leqslant 2q$. We have $p \geqslant q \geqslant 3$, implying $p^2 > 2q + 1$. With $p \leqslant 2q$ this gives $1 \leqslant [g(q)]_p = [[g(q)]]_p$. On the other hand, $p \geqslant q$, and thus A, $B \leqslant 1$ and

$$A + B \leqslant 2 \leqslant [[g(q)]]_p + 1.$$

Hence, by 5.3(a),

$$A + B \leqslant [[g(q)]]_p.$$

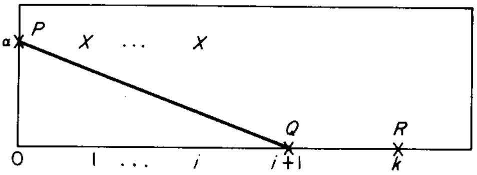
$p > 2q + 3$. We recall the polynomial (1.1) of Remark 1.12, which has rational roots precisely when $R_k(x)$ has, namely $f(x) = \Sigma_{i=0}^{k} c_i x^i$, where

$$c_0 = \binom{Y}{z} = \frac{Y(Y - 1) \ldots (Y - z + 1)}{z(z - 1) \ldots 1},$$

$$c_1 = k\binom{Y - 1}{z - 1} = k\frac{(Y - 1)(Y - 2) \ldots (Y - z + 1)}{(z - 1)(z - 2) \ldots 1},$$

$$c_k = \binom{Y - k}{z - k}.$$

Suppose that, in the notation of (5.2), we have $B > 0$. Then $p^\alpha \parallel Y - i$ for some odd α and odd i with $Y - i > Y - k$. But $p > 2q + 3 \geqslant z$, so i is unique and p does not divide $z!$. Thus the Newton polygon of $f(x)$ for the prime p has the form PQR below:



(5.3)

Since $f(x)$ is assumed to have no irrational root, the slope $(-\alpha)/(i+1)$ of PQ must be an integer, by Theorem 1.11 (a vital step in our argument). But this implies the contradiction that i is even. So B must be zero after all. But now, from $p > 2q + 3$, we have $[[g(q)]]_p = 0$ and $A \leqslant 1$, whence

$$A + B \leqslant [[g(q)]]_p + 1.$$

With 5.3(a) this implies $A + B = 0$. Thus the proof of Theorem 5.2 is complete.

The Contradiction for $q \geqslant 85$ ($k \geqslant 171$). For Cases 3 and 4 let

$$2^\alpha, 3^\beta \parallel (2q+3)! \qquad \text{and} \qquad 2^\gamma, 3^\delta \parallel \Pi a_i b_j.$$

Then, by Theorem 5.2,

$$\Pi a_i b_j \parallel 2^{\gamma-\alpha} 3^{\delta-\beta} (2q+3)!(2q+1)(2q+3) \prod_{\sqrt{2q}<p<q} p^2. \tag{5.4}$$

Further, we shall assume

$$q \geqslant 85, \qquad \text{so that } \sqrt{2q} > 13,$$

and, by (3.6),

$$\prod_{\sqrt{2q}<p<q} p^2 < 3^{2q}/G, \qquad G = \prod_{p<14} p^2, \tag{5.5}$$

where we may replace 3^{2q} by e^{2q} when $0 < q < 10^8$. Bounds for α, β are, from $L = 2q + 3$ in 2.2,

$$\begin{aligned} \alpha &\geqslant 2q + 2 - \log_2 (q+2), \\ \beta &\geqslant q + \tfrac{1}{2} - \log_3 (q+2). \end{aligned} \tag{5.6}$$

The second bound includes the observation that $\log_3 2 < 1$. For bounds on γ, δ we need to consider $a_1 \ldots a_q$ and $b_1 \ldots b_q$ separately.

Let $p = 2$. Since N, $Y - 1$ have opposite parity (see (5.1A)), one of the products $(N+2)(N+4) \ldots (N+2q)$ and $(Y-1)(Y-3) \ldots (Y-2q+1)$ consists of odd numbers; the other of even. Hence the bound on γ comes from squarefree numbers on just q consecutive *even* integers. Thus 2.4(c) applies with $L = q$. On the other hand, for $p = 3$ we can apply 2.4(b) with $L = q$ and double the given bound. The result is

$$\begin{aligned} \gamma &\leqslant \frac{2q}{3} + 1 + \tfrac{1}{3} \log_2 q, \\ \delta &\leqslant \tfrac{1}{2} q + \tfrac{1}{2} + \log_3 (2q+1). \end{aligned} \tag{5.7}$$

We need all $2q$ squarefree integers to be distinct. To ensure this we use 2.3(c) with: for Case 3, $L = 2k - 2$, $M = n + 1$; for Case 4, $L = 2k$, $M = 2n + 1$. Throughout, $n \geqslant k^2$ implies $M \geqslant L^2/4$, as required. Thus, from Theorem 2.5,

$$(2q)!\,(\tfrac{3}{2})^{2q} < a_1 \ldots a_q b_1 \ldots b_q \qquad (q \geqslant 32). \tag{5.8}$$

Combining this with (5.4) to (5.7), we deduce

$$(\tfrac{27}{16})^{q/6} < 32(q + 2)^{8\frac{1}{3}}/G \qquad (q \geqslant 85) \tag{5.9}$$

which gives a contradiction for $q \geqslant 380$. To extend this downwards we replace 3^{2q} by e^{2q} in (5.5); then (5.4) to (5.8) give

$$\left(\frac{3}{e}\right)^{2q}\left(\frac{27}{16}\right)^{q/6} < 32(q + 2)^{8\frac{1}{3}}/G \qquad (85 \leqslant q < 10^8).$$

This is a contradiction for $q \geqslant 85$ ($k \geqslant 171$).

The Range $3 \leqslant k \leqslant 170$. We need to distinguish again the four cases in (5.1A). The proof in Theorem 5.2 that $A + B = 0$ for $p > 2q + 3$ goes through for $p > z$, and so

$$p \nmid \Pi a_i b_j \qquad \text{if } p > z. \tag{5.10}$$

Thus we have once more an inequality of the form

$$2q \leqslant 2^{r-1} + Bp_r \qquad (r > 1), \tag{5.11}$$

where, by (5.10) with 2.4(a) and 5.3(a), we may set

$$Bp_r = \sum_{p_r \leqslant p \leqslant z} (2\lceil q/p \rceil - ([[g(q)]]_p \bmod 2)). \tag{5.12}$$

Then (5.11) is contradicted by $8 + B_7 < 2q$ for $9 \leqslant q \leqslant 84$ in all four cases. Also, $2 + B_3 = 3 < 2q$ for 3_{2q} with $q = 2$. The remaining values of q are either settled by $4 + B_5 < 2q$ or are counted as exceptional and treated in Section 6. The table below is a convenient reference:

Case	q: $4 + B_5 < 2q$	Exceptional values of q
3_{2q}	3, . . . , 8	None
3_{2q+1}	4, . . . , 8	1, 2, 3
4_{2q}	4, 5, 7, 8	2, 3, 6
4_{2q+1}	7	1, 2, . . . , 6, 8

6. Exceptional Values of k: Cases 1, 3 and 4

In this section we eliminate the possibility of tight t-designs in complex or quaternionic projective spaces for certain low values of t. As described in Section 1, this comes down to proving that a certain product D of integers cannot be a perfect square by considering the squarefree parts a_i of its factors:

$$N + r_i = a_i x_i^2, \qquad i = 1, 2, \ldots, \quad 0 < r_1 < r_2 < \ldots . \tag{6.1}$$

For D and the details of (6.1) see (3.1), (3.2) in Case 1 and (5.1), (5.2) in Cases 3, 4. The a_i will always be distinct, under our assumption $n \geqslant k^2$ (1.14 with Theorem 2.3), but here we switch to congruence techniques plus the Newton polygon (see 1.10). First, a simple but vital remark which we often use implicitly:

6.1 Remark

(a) For prime p and integers n, i: $p \mid n + i$ if and only if $p \mid n + 1 + p$.

(b) With prime divisors restricted to 2, 3 there are just four distinct squarefree integers 1, 2, 3, 6; similarly for other prime pairs.

(c) With prime divisors restricted to 2, 3, 5 the number of distinct squarefree integers is eight, and their product is $2^4 \cdot 3^4 \cdot 5^4$; similarly for other triples of primes.

6.2 Diophantine Equations. For integers x, y, z, r we write

$$x^y z \bmod r$$

to mean that the equations $R = xA^2$, $R + y = zB^2$ can have no integer solutions R, A, B because they have no solution when reduced modulo r. We say $(a_1, a_2, \ldots, a_u)$ *fails mod* r if the Diophantine equations $N + r_i = a_i x_i^2$, $1 \leqslant i \leqslant u$, have no solution $N, x_1, \ldots, x_u$ when reduced modulo r. We give two examples of how the non-existence of a solution is established in this context.

Example 1: $0^2 3 \bmod 7$. The equations $R = 0$, $R + 2 = 3B^2$ imply $3B^2 = 2$, which has no solution mod 7, since 2 is a square and 3 is a non-square mod 7 (see 6.3 below). It follows of course that $7^2 3 \bmod 7$, $14^9\ 10 \bmod 7$, and so on.

Example 2: $6^9 3 \bmod 8$. The equations $R = 6A^2$, $R + 9 = 3B^2 \bmod 8$ imply $6A^2 + 1 = 3B^2$. From 6.3, the left-hand side equals 1 or 7 mod 8, whereas the right-hand side equals 0, 3, or 4.

6.3 The Non-zero Squares (□) mod r

r	□	r	□	r	□
3	1	7	1, 2, 4	13	1, 3, 4, 9, 10, 12
4	1	8	1, 4	16	1, 4, 9
5	1, 4	11	1, 3, 4, 5, 9		

6.4 Useful Cases of $x^y z \bmod r$

mod 3: $0^1 2$, $0^2 1$, $2^2 0$.

mod 5: $0^1 2$, $0^1 3$, $2^1 0$, $3^1 0$, $0^2 1$, $1^2 0$.

mod 7: $0^1 3$, $0^1 5$, $0^1 6$, $1^1 0$, $2^1 0$,
$0^2 3$, $0^2 5$, $0^2 6$, $2^2 0$, $1^2 0$.

6.5 Lemma. *The Diophantine equation*

$$x^4 - dy^2 = 1 \tag{6.2}$$

has no solution in positive integers x, y *for* $d = 3, 10, 30$, *and unique solutions* $(3, 4)$ *if* $d = 5$, $(2, 1)$ *if* $d = 15$.

Proof. Such equations, with $d \geqslant 1$ and squarefree, have at most two solutions in integers [19, p. 61]. Since $x = 1$, $y = 0$ is always a solution, there is at most *one* solution in *positive* integers; this takes care of cases $d = 5, 15$. For the rest, suppose that x, y is a solution and that $E_0 = a + b\sqrt{d}$ is the basic unit in $Q(\sqrt{d})$, with norm $N(E_0) = a^2 - b^2 d = \pm 1$. Then $x^2 + y\sqrt{d}$ is a unit and, from [19, p. 61], we have

$$x^2 + y\sqrt{d} = E^s,$$

where s is odd, and *either* $E = E_0$ (and then $N(E_0) = 1$ since $1 = x^4 - dy^2 = (N(E_0))^s$) *or* $E = E_0^2$. Further [18, p. 48, Eqn (66)], for some integer M,

$$x^2 + 1 = (u + 1)M^2, \qquad \text{where } E = u + v\sqrt{d}. \tag{1}$$

If $d = 3$ we have $E_0 = 2 + \sqrt{3}$, $E_0^2 = 7 + 4\sqrt{3}$. Hence, by (1), $x^2 + 1 = 4M^2$ or $x^2 + 1 = 8M^2$, which both fail mod 4. If $d = 10$ then $E_0 = 3 + \sqrt{10}$, $N(E_0) = -1$, $E_0^2 = 19 - 6\sqrt{10}$, so we have only to consider the equation $x^2 + 1 = 20M^2$ from (1). But this too fails mod 4. If $d = 30$ then $E_0 = 11 + 2\sqrt{30}$, $E_0^2 = 241 + 44\sqrt{30}$ and (1) gives $x^2 + 1 = 12M^2$, which fails mod 4, or $x^2 + 1 = 242M^2$, which this time fails mod 11.

6.6 Theorem. *With $n + i = a_i x_i^2$ ($i, n \geqslant 1$), a_1 squarefree (as in Case 1), and prime divisors of the a_i restricted to* 2, 3, 5, *every sequence* $(a_1, a_2, \ldots)$ *of distinct a_i is amongst those listed below*:

(a) *Pairs*: (1, 2), (1, 5), (1, 10), (2, 1), (2, 3), (3, 1), (5, 1), (5, 6), (6, 1), (10, 1), (15, 1), (30, 1).
(b) *Triples*: (1, 2, 3), (1, 5, 6) (*possibly infinite families*), (2, 1, 10) *if* $n = 7$, (2, 3, 1) *if* $n = 1$, (3, 1, 2) *if* $n = 47$, (3, 1, 5) *if* $n = 2$.
(c) (2, 3, 1, 5, 6) *and subsequences* (2, 3, 1, 5), (3, 1, 5, 6) (*each for unique* n).

Proof. Without loss of generality, we write (a_1, a_2) rather than (a_i, a_{i+1}), and similarly for triples.

(a) *Pairs*. Of the pairs allowed by $a_1 \mid 30$, $a_2 \mid 30$ with the a_i coprime, 6.4 rules out all except those cited.

(b) *Triples*. We start with those triples (a_1, a_2, a_3) for which (a_1, a_2) and (a_2, a_3) are allowed by part (a) and, following Remark 6.1, hcf$(a_1, a_3) \leqslant 2$. They fall into four groups as below:

(1) (5, 6, 1): this is impossible, by $5^2 1$ mod 5.
(2) (2, 3, 1), (3, 1, 2). With $n + 1 = 2x$ in either triple we obtain $x(x + 1)(2x + 1) = 6M^2$ ($M \in \mathbb{N}$). This is Lucas' Pyramid problem [21, p. 258, Theorem 4], whose positive integer solutions are $x = 1, 24$, giving respective triples (2, 3, 1), (3, 1, 2).
(3) Triples with $a_2 = 1$. Besides (3, 1, 2), dealt with above, we obtain (2, 1, 5), (2, 1, 10), (3, 1, 5), (3, 1, 10), (5, 1, 2), (6, 1, 2), (6, 1, 10), (10, 1, 2), (15, 1, 2), (30, 1, 2). All are covered by Lemma 6.5. For example, (10, 1, 2) gives $B^2 - 1 = 10A^2$, $B^2 + 1 = 2C^2$ ($A, B, C \in \mathbb{Z}$), whence $B^4 - 5(AC)^2 = 1$, with solution $B = 3$ yielding no such triple. In Fact, $B = 3$ gives (2, 1, 10), with $n = 7$.
(4) (1, 2, 3), (1, 5, 6). We expect the methods of Ljunggren in [18, 19] to show that there is at most one solution for n in both cases, but we will pursue this elsewhere, since such a result is not needed here because of Corollary 6.8.

6.7 Remark. All pairs of Theorem 6.6 occur, and hence, by the theory of Pellian equations $x^2 - dy^2 = C$, they occur for infinitely many values of n. See, e.g. [23, p. 215, Problem 2]. Of course $3B^2 - 2A^2 = 1$ from the pair (2, 3) is viewed as $x^2 - 6y^2 = 3$.

6.8 Corollary. *In Case* 1, *if every a_i divides* 30, *then*:
(a) *every possible triple contains a* '1';
(b) *for $n > 2$ there are no* 4-*tuples*.

In the following, we will sometimes write 'pd' for 'prime divisor'.

Case 1. See (3.1), (3.2) for the form of D below. We note that $n \geqslant k^2 \geqslant 9$.

$k = 3$. $D = (n + 1)(n + 3)$ is a square. Let $s = n + 2$. Then $s^2 - 1$ is a square: contradiction.

$k = 4$. $D = 5(n + 1)(n + 2)(n + 3)(n + 4)$. By Remark 6.1, the a_i have pd's restricted to 2, 3, 5 so by Corollary 6.8(b) there can be no 4-tuple of distinct a_i. Hence this case cannot occur.

$k = 5$. $D = (n + 1)(n + 2) \times (n + 4)(n + 5)$. By Remark 6.1 the four distinct a_i must be 1, 2, 3, 6 in some order. Now, 6.8(b) does not apply, as the a_i are not in four consecutive integers. However, 6.1 limits the orders to 2316, 6132, 3261, 1623, and each such order gives a pair (1, 6) or (3, 2), which is impossible by Theorem 6.6.

$k = 6$. $D = 7(n + 1)(n + 2) \ldots (n + 6)$. By 6.1, since D is a square, the pd's of the a_i do not exceed 7, and 7 divides exactly one a_i. Furthermore,

(1) $5 \mid a_1$ and $5 \mid a_6$;

(2) if $3 \mid a_2$ then $3 \mid a_5$.

Since by 6.8(b) no four consecutive a_i have pd's restricted to 2, 3, 5, we must have $7 \mid a_3$ or $7 \mid a_4$. With (1), Theorem 6.6(a) implies $a_5 = 1$ and hence that $a_2 = 6$. But this contradicts (2).

$k = 7$. $D = (n + 1)(n + 2)(n + 3) \times (n + 5)(n + 6)(n + 7)$. By Remark 6.1 the a_i have pd's restricted to 2, 3, 5. Hence by Corollary 6.8(b) two of the a_i must be 1: contradiction.

$k = 9$. $D = (n + 1)(n + 2)(n + 3)(n + 4) \times (n + 6)(n + 7)(n + 8)(n + 9)$. Here the possible pd's are 2, 3, 5, 7 and, by Remark 6.1(a), Πa_i divides $2^4 \cdot 3^2 \cdot 5^2 \cdot 7^2$. Since there are eight distinct a_i, Remark 6.1(c) shows that each of 2, 3, 5, 7 divides some a_i. Now, either $7 \mid a_1$, $7 \mid a_7$ *or* $7 \mid a_2$, $7 \mid a_8$.

Let $7 \mid a_1$. By Remark 6.1(a), 5 divides $a_2 a_3 a_4$ so, invoking Theorem 6.6(b) and noting that $n \geqslant k^2 = 81$, we see that $(a_2, a_3, a_4) = (1, 5, 6)$. But now (a_1, a_3) fails mod 7, because of $0^2 5$ mod 7.

Let $7 \mid a_2$. We note this time that 5 divides $a_5 a_6 a_7$ and so $(a_5, a_6, a_7) = (1, 5, 6)$, whence $5 \mid a_3$. But now, Theorem 6.6(a) and distinctness of the a_i allow no possible pairs (a_3, a_4), and so the proof for Case 1 is complete.

CASES 3 AND 4. Here we have, up to multiplication by a square,

$$D = (\text{squarefree part of } g(q)) \times (N + 2)(N + 4) \ldots (N + 2q)$$
$$\times (N + 2q + \gamma)(N + 2q + \gamma + 2) \ldots (y - 1), \quad (6.3)$$

where the two sets of q factors are arithmetic progressions of modulus 2, between which there is a 'gap' $\gamma = 1, 3, 3, 5$, according as we are in Case 3_{2q}, 3_{2q+1}, 4_{2q} or 4_{2q+1} respectively. We note that N is always even in Case 4. Further details are given in (5.1A), including the upper bound z for the size of prime divisors of the a_i and b_i. As in Case 1, we require a lemma on Diophantine equations.

6.9 LEMMA. *The Diophantine equation*

$$Ax^4 - By^2 = 4 \quad (6.4)$$

has a unique solution x, y in positive integers for the given values of A, B in the following 4-tuples (A, B, x, y): (1, 77, 3, 1), (9, 5, 1, 1), (25, 21, 1, 1), (49, 5, 1, 3), (121, 13, 1, 3), (169, 165, 1, 1).

PROOF. Suppose that (i) the *second degree* equation $Ax^2 - By^2 = 4$ has a solution in odd positive integers x, y, the least such solution being (a, b), and (ii) $a = h^2$ ($h \in \mathbb{N}$) but $Ah^4 - 3$ is not a fourth power. Then by a result of Ljunggren [20, p. 150, Theorem 1] the fourth degree equation (6.4) has $x = h$ as unique solution. To establish the present lemma we simply use the given solutions of (6.4) to verify conditions (i) and (ii) in each stated case of (A, B). For example, $1 \cdot x^2 - 77y^2 = 4$ has least solution $a = 9 = 3^2$ and $1 \cdot 3^4 - 3$ is not a fourth power; therefore $x = 3$ is the unique solution of $x^4 - 77y^2 = 4$.

6.10 THEOREM. *Let N be an odd positive integer with $N + 2i = a_i x_i^2$, a_i squarefree, $1 \leqslant i \leqslant L$, $L > 1$. If no prime divisor of an a_i exceeds* 13, *then any sequence* $(a_1, a_2, \ldots)$ *of distinct a_i is amongst those below*:

(a) *Pairs* (1, 3), (3, 5), (5, 7), (7, 1), (1, 11), (11, 13), (13, 15), (3, 77), (5, 143), (7, 65), (13, 7), (33, 35), (273, 11).

(b) *Sequences of consecutive elements of* (3, 5, 7, 1, 11, 13, 15) ($N \leqslant 9$).

REMARK. Each pair occurs for infinitely many values of N (cf. Remark 6.7).

PROOF. We note the following facts about (a_i, a_{i+1}):
(1) a_i, a_{i+1} are coprime;
(2) $a_{i+1} = a_i + 2 \pmod 8$ [since $x_i^2 = 1$, x_i being odd];
(3) a_i is a square modulo the prime p if and only if $N + 2i$ is.

Pairs: *the case* $a_1 a_2 | 3.5.7.11$. The following table of possible values of a_i not divisible by 13 will be useful:

$a_i \equiv 1 \pmod 8$:	1	105	33	385
$a_i \equiv 3 \pmod 8$:	3	35	11	1185
$a_i \equiv 5 \pmod 8$:	5	21	77	165
$a_i \equiv 7 \pmod 8$:	15	7	55	231

(6.5)

Note that the integers in the second column have a common factor 7, while those in the last two columns are divisible by 11. We thus see that conditions (1) and (2) allow the pairs given in part (a) of the theorem and, in addition, (5, 231), (11, 21), (15, 1), (21, 55), (77, 15), (165, 7), (231, 1), which fail mod 3; (1, 35), (1, 1155), (11, 5), (55, 1), (105, 11), which fail mod 5; (7, 33), (385, 3), which fail mod 7.

Pairs: *the case* $13 | a_1 a_2$. For $i = 1, 2$, if $13 | a_i$ then a_{3-i} is a non-square mod 13 (since $a_{3-i}B^2 = \pm 2$ for some integer B); thus $a_{3-i} \in \{5, 7, 11, 15, 21, 33, 385, 1155\}$. We note that if 13λ is congruent mod 8 to 1, 2, 3, 4, 5, 6, 7 then λ is congruent to 5, 2, 7, 4, 1, 6, 3 respectively. With (2), this determines the λ column in the tables below. The possible (a_1, a_2) are determined by (1) and (65) above:

$a_1 = 13\lambda$

a_2	λ (mod 8)	(a_1, a_2)	Status
5	7	(13·7, 5)	$1^2 0$ mod 5
		(13·231, 5)	$0^2 5$ mod 7
7	1	(13, 7)	Occurs
		(13·33, 7)	$0^2 1$ mod 3
11	5	(13·5, 11)	$0^2 1$ mod 5
		(13·21, 11)	Occurs
15	1	(13, 15)	Occurs
21	7	(13·55, 21)	$0^2 1$ mod 5
33	3	(13·35, 33)	$0^2 5$ mod 7
385	3	(13·3, 385)	$1^2 0$ mod 5
1155	5	None	

$a_2 = 13\lambda$

a_1	λ (mod 8)	$(a_1 a_2)$	Status
5	3	(5, 13·3	$2^2 0$ mod 3
		5, 13·11)	Occurs
7	5	(7, 13·5	Occurs
		(7, 13·165)	$0^2 3$ mod 7
11	1	(11, 13)	Occurs
		(11, 13·105)	$2^2 0$ mod 3
15	5	(15, 13·77)	$1^2 0$ mod 7
21	3	(21, 13·11)	$0^2 3$ mod 7
33	7	(33, 13·7)	$0^2 1$ mod 3
385	7	None	
1155	1	(1155, 13)	$0^2 1$ mod 3

This completes the proof of part (a).

(b) *u-tuples*, $u \geqslant 3$. We consider first the triples (a_1, a_2, a_3) for which (a_1, a_2) and (a_2, a_3) are allowed by part (a). They fall into two groups:

(1) The following 'failures'; mod 3, (3, 5, 143), (7, 1, 3), (13, 7, 1); mod 5, (5, 7, 65), (13, 7, 65); mod 7 (1, 3, 77), (11, 13, 7), (273, 11, 13).

(2) The six triples (1, 3, 5), (3, 5, 7), (5, 7, 1), (7, 1, 11), (1, 11, 13), (11, 13, 15). By Lemma 6.9, each is realized uniquely, and within the consecutive odd integers 3, 5, . . . , 15. For example, the triple (3, 5, 7) involves $5B^2 - 2 = 3A^2$, $5B^2 + 2 = 7C^2$ for integers A, B, C; hence $25B^4 - 21(AC)^2 = 4$, with unique solution $B = 1$, $N + 4 = 5B^2 = 5$.

To complete the proof of part (b), we observed that any u-tuple ($u \geqslant 4$) that occurs contains a triple, which must be one of those listed in (2).

6.11 Remark. Theorem 6.10 applies to both a_i and b_i in Cases 3 and 4, and their pd's are bounded by the z of (5.1A) (see (5.10)).

6.12 Corollary. *Cases* 3 *and* 4 *with* $3 \leqslant q \leqslant 6$ *cannot occur.*

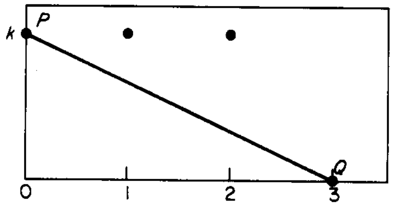
Proof. Each case cited requires a triple of distinct a_i (or b_i) with N odd, $N \geqslant k^2 \geqslant 36$. But $z \leqslant 15$ by (5.1A), so Theorem 6.10 rules out all such triples.

The Remaining Cases 3 and 4. We give each time the upper bound z for prime divisors of the a_i, b_i.

Case 3_{2q+1}, $q = 1$. $D = 2 \cdot 3(Y - 4)(Y - 1)$, $z = 3$. Clearly $a_1 b_1 = 6$, so by $3^3 2$ mod 3 and $1^3 6$ mod 3 there are just two cases of (a_1, b_1) to consider.

(1) (2, 3). Here $Y - 4 = 2A^2$, $Y - 1 = 3B^2$ for integers A, B. We investigate the prime decomposition of $Y - 2$. Working mod 8, we have $A^2 \equiv 0$, 1 or 4 (see 6.3) so $Y - 4 = 2A^2 \equiv 0$ or 2, and $Y - 1 \equiv 3$ or 5. But now $Y - 1 = 3B^2$ implies $Y - 1 \equiv 3$, or $Y - 2 \equiv 2$, and therefore $2 \parallel Y - 2$. Further, 3 divides $Y - 1$, so does not divide $Y - 2$.

For a prime $p > 3$, let $p^\lambda \parallel Y - 2$. Then the Newton polygon (see 1.10) with respect to p of $f(x) = \Sigma_{i=0}^{3} \binom{3}{i}\binom{Y-i}{3-i}x^i$ is the line segment PQ below:



Since $f(x)$ is assumed to have only rational roots, the slope $-\lambda/3$ is integral by Theorem 1.11. We have proved that $Y - 2 = 2W^3$ for some integer W, and so $2 = (Y - 2) - (Y - 4) = 2W^3 - 2A^2$. From Hemer's table [14, p. 75] this has no solution with $W > 1$, hence case (1) cannot arise.

(ii) (6.1). Here $Y - 4 = 6A^2$, $Y - 1 = B^2$ for integers A, B. Proceeding as in (i), we find that $Y - 2 \equiv 0 \pmod 8$, so $2^\lambda \parallel Y - 2$, $\lambda \geqslant 3$. If $\lambda > 3$, the Newton polygon with respect to the prime $p = 2$ comes from the convex hull of points $(0, \lambda)$, $(1, \lambda - 1)$, $(2, \lambda)$, $(3, 0)$, and so is a line segment of slope $-\lambda/3$. Hence $3 \mid \lambda$.

If $p > 3$, $p^\lambda \parallel Y - 2$, then $3 \mid \lambda$ as in (i). Thus $Y - 2 = W^3$ ($W \in \mathbb{N}$) and $1 = (Y - 1) - (Y - 2) = B^2 - W^3$. But the latter has no solution with $W < 2$ (see [14, p. 74], or [21, p. 247, Theorem 5]). Thus (ii) cannot arise, and this case is eliminated.

Case 4_{2q+1}, $q = 1$. $D = 3(Y - 6)(Y - 1)$, Y even, $z = 5$. Here $a_1 b_1$ equals 3 or 3.5^2. Now $1^5 3$ mod 5, $3^5 1$ mod 3, $5^5 15$ mod 3 together imply $(a_1, b_1) = (15, 5)$, hence $Y - 6 = 15A^2$ and $Y - 1 = 5B^2$ for integers A, B. As before, we investigate the prime decomposition of $Y - 2$. We note that B is odd, since Y is even, so $B^2 \equiv 1 \pmod 8$. Thus $Y - 2 = 5B^2 - 1 \equiv 4 \pmod 8$, and $2^2 \,\|\, Y - 2$.

Now consider the prime 3. If $3 \mid Y - 2$ then $5B^2 - 1 \equiv 0 \pmod 3$, implying the contradiction $B^2 \equiv -1 \pmod 3$. Hence 3 does not divide $Y - 2$. Also, 5 divides $Y - 1$ so does not divide $Y - 2$. For a prime $p > 5$ with $p^\lambda \,\|\, Y - 2$, the Newton polygon with respect to p comes from points $(0, \lambda)$, $(1, \lambda)$, $(2, \lambda)$, $(3, 0)$, and shows that $3 \mid \lambda$. We may now conclude that $Y - 2 = 4W^3$ ($W \in \mathbb{N}$), and so we can write $4 = (Y - 2) - (Y - 6) = 4W^3 - 15A^2$, $A = 2C$, for integers A, C, W, whence $1 + 15C^2 = W^3$. But this last equation has only the trivial solution, as we now prove, by techniques described in [21, pp. 241–242].

In the quadratic field $Q(\sqrt{-15})$ we have

$$(1 + C\sqrt{-15})(1 - C\sqrt{-15}) = W^3.$$

Since 3 is coprime to the class number, 2, and the left-hand factors are coprime (W being odd), it follows that

$$1 + C\sqrt{-15} = (P + Q\sqrt{-15})^3$$

for integers P, Q. Thus $1 = P(P^2 - 45Q^2)$ and P is a unit ± 1 in Z. If $P = -1$ then $45Q^2 = 2$, a contradiction. If $P = 1$ we obtain the trivial solution $Q = 0 = C$, $W = 1$.

Case 3_{2q+1}, $q = 2$. $D = 2{\cdot}3{\cdot}5(N + 2)(N + 4) \times (N + 7)(N + 9)$, $z = 5$. Here, $a_1 a_2 b_1 b_2 = 2{\cdot}3{\cdot}5$ and so Theorem 6.10 leaves four possible cases of $(a_1, \ldots, b_2)$, for each of which we now give a contradiction (unknown a_i, b_i are signified by dashes):

N odd 3 5 _ _: no place for 1, by $3^5 1$ mod 3 and $3^7 1$ mod 7;

1 3 _ _: no place for 5, by $1^7 5$ mod 5 and $3^3 5$ mod 3.

N even _ _ 3 5: no possible a_1, by $1^7 5$ mod 5 and $2^7 5$ mod 7;

_ _ 1 3: no place for 5, by $5^3 1$ mod 5 and $5^5 3$ mod 3.

Case 4_{2q}, $q = 2$. $D = 2(N + 2)(N + 4) \times (N + 7)(N + 9)$, N even, $z = 6$. We have $a_1 a_2 b_1 b_2 = 2{\cdot}3^2{\cdot}5^2$, $3 \mid a_2$ and $3 \mid b_1$. Now, since N is even, Theorem 6.10 shows that $(b_1, b_2) = (3, 5)$ and hence that $5 \mid a_2$. This leaves two cases of (a_1, a_2): $(2, 15)$, contradicted by $2^2 0$ mod 3, and $(1, 30)$, contradicted by $1^2 0$ mod 5.

Case 4_{2q+1}, $q = 2$. $D = 2{\cdot}5(N + 2)(N + 4) \times (N + 9)(N + 11)$, N even, $z = 7$. We obtain $a_1 a_2 b_1 b_2 \mid 2{\cdot}3^2{\cdot}5{\cdot}7^2$ and

(1) if 3 occurs then $3 \mid a_1$ and $3 \mid b_2$,

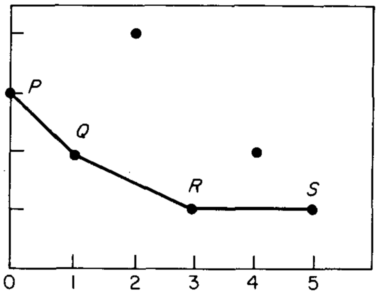
(2) if 7 occurs then $7 \mid a_1$, $7 \mid b_1$ or $7 \mid a_2$, $7 \mid b_2$.

Now, if $a_1 a_2 b_1 b_2 = 2{\cdot}3^2{\cdot}5{\cdot}7^2$ then $(b_1, b_2) = (1, 3)$ by (1) and Theorem 6.10, which contradicts (2). So we have the following cases of $(a_1, \ldots, b_2)$, each of which we rule out by modular considerations

(i) $\Pi a_i b_i = 2{\cdot}3^2{\cdot}5$. 6 5 1 3: $6^2 5$ mod 5; 15 2 1 3: $15^9 3$ mod 5.

(ii) $\Pi a_i b_i = 2{\cdot}5{\cdot}7^2$. 1 14 5 7: $1^7 5$ mod 5; 14 5 7 1: $5^7 1$ mod 5.

A third and final possibility is 3 5 2 7 1. Here we have $Y - 1 = A^2$, $Y - 3 = 7B^2$, $Y - 8 = 2C^2$, $Y - 10 = 35E^2$, for integers A, B, C, E. The squares mod 8 are 0, 1, 4 so $Y - 8 \equiv 0$ or 2 and $A^2 = Y - 1 \equiv 1 \pmod 8$. Hence $2^3 \mid Y - 2$. What is $Y - 2$ mod 16? Suppose that $2^3 \,\|\, Y - 2$. Then the Newton polygon with respect to 2 is $PQRS$ below:



Since QR has non-integral slope $-1/2$, our assumption $2^3 \parallel Y - 2$ is false, whence $Y - 2 \equiv 0 \pmod{16}$. But now, $2B^2 = Y - 8 \equiv 10 \pmod{16}$, which is contradiction, since the squares mod 16 are 0, 1, 4, 9.

Case 4_{2q+1}, $q = 8$. $D = 2 \cdot 5 \cdot 11 \cdot 13 \cdot 17(N+2)(N+4)\ldots(N+16) \times (N+21)(N+23)\ldots(N+35)$, N even, $z = 19$. Referring to (5.11), (5.12) we have $4 + B_5 = 16 = 2q$, and so, in particular $7^4 \parallel \Pi a_i b_i$. But the form of D renders this impossible, and the proof of the main result of this paper is complete.

7. Appendix: The Proof of Theorem 1.15

Write $L = M + r - 1$. Then 1.15 is equivalent to:

7.1 Theorem. *Let L, r be positive integers with $L \geqslant 3r - 1$, $r \geqslant 63$. Then $\binom{L}{r}$ has a prime divisor $p > 2r$.*

Proof. We proceed in three stages:

(1) *The case $L > r^{3/2}$.* This is itself split into the following:
(a) $L \geqslant r^2$, $r \geqslant 63$;
(b) $L \geqslant r^{3/2}$, $r \geqslant 575$;
(c) $r^{3/2} \leqslant L \leqslant r^2$, $63 \leqslant r \leqslant 575$.
The finine number of cases (r, L) in (c) is verified by computer calculation. For the rest, we compute the bounds

$$\Pi(x) \leqslant \begin{cases} x/4, & x \geqslant 126, \\ x/6, & x \geqslant 1150, \end{cases}$$

as follows. From [25, p. 69, Theorem 2] we have $\Pi(x) < x/(\log x - 3/2)$ for $x > e^{3/2}$. Hence, for a positive integer s, $\Pi(x) < x/s$ if $(\log x - 3/2) > s$. The latter condition holds for $s = 4, 6$, if x exceeds 245, 1809 respectively, and these limits reduce to 126, 1150 by direct calculation of $x/s - \Pi(x)$. Now (a) and (b) follow from the following lemma, with $\beta = 1/4$ and $1/6$ respectively.

Lemma. *If $\Pi(x) \leqslant \beta x$ for $x \geqslant 2r_0$, then Theorem 7.1 is true for all (r, L) with $r \geqslant r_0$* and $L \geqslant r^{1/(1-2\beta)}$.

Proof. Suppose that Theorem 7.1 fails for some (r, L) allowed by the lemma; that is, all prime divisors p of $\binom{L}{r}$ satisfy $p \leqslant 2r$. Using a technique of Erdös, with his result that if $p^\alpha \mid \binom{L}{r}$ then $p^\alpha \leqslant L$ [9], we have

$$\left(\frac{L}{r}\right)^r < \binom{L}{r} \leqslant L^{\Pi(2r)} \leqslant L^{2r\beta} \qquad (2r \geqslant 2r_0).$$

Hence the contradiction $L < r^{1/(1-2\beta)}$.

(2) *The case* $12r \leqslant L < r^{3/2}$. Suppose that $12r \leqslant L < r^{3/2}$, but that every prime divisor p of $\binom{L}{r}$ satisfies $p \leqslant 2r$. Then we have:

$$
\begin{aligned}
4^{2r+\sqrt{L}} &> \binom{L}{r}, && \text{by adapting an argument of Erdös [9];}\\
&\geqslant \binom{12r}{r}, && \text{as } L \geqslant 12r;\\
&= \binom{2r}{r}\,{}_r(12r)/{}_r(2r) > 4^r \cdot 6^r/2r.
\end{aligned}
$$

Hence $4^{\sqrt{L}} > (\frac{3}{2})^r/2r > \alpha^r$ ($r \geqslant 100$), where $\alpha = 3/(2^{13/12})$. By taking logarithms we obtain $r \log \alpha < \sqrt{L} \log 4 < r^{3/4} \log 4$, as $L < r^{3/2}$. This is the required contradiction, for $r > 250$. It remains to verify by calculation that 7.1 holds for $12r \leqslant L < r^{3/2}$, $63 \leqslant r \leqslant 250$.

(3) *The case* $3r - 1 \leqslant L < 12r$. From [24, p. 433, Eqn (3)] we have that, for $x \geqslant 118$, there is a prime p with

$$x < p \leqslant 12x/11. \tag{7.2}$$

Since $r \geqslant 63$ we may apply (7.2) to $x = L - r + 1 \geqslant 2r \geqslant 126$, obtaining $L - r + 1 < p < 12(L - r + 1)/11 \leqslant L$ (as $r \geqslant L/12$). Since $L \geqslant 3r - 1$, we have the desired prime divisor $p > 2r$ of $\binom{L}{r}$, and this completes the proof of 7.1.

Acknowledgements

It is a pleasure to record our thanks to both referees for their valuable comments: also, to the colleagues R. Tijdeman and M. Coster of one of the referees, for a sharpening of the originals of Theorems 2.2–2.4, and for the suggestion to add to the rules for eliminating pairs and triples in Section 6, an enumeration of those which *are* possible. This inspired the application of Diophantine equations in Lemma 6.5 to Theorem 6.6, and 6.9 to 6.10, leading to a shorter and more readable treatment of the exceptional values of k.

E. Bannai was supported, in part, by NSF grants MCS-830826 and DMS-8503761.

References

1. E. Bannai and R. M. Damerell, Tight spherical designs, I. *J. Math. Soc. Japan* **31** (1979), 199–207.
2. E. Bannai and R. M. Damerell, Tight spherical designs, II. *J. London Math. Soc.* (2) **21** (1980), 13–30.
3. E. Bannai and S. G. Hoggar, On tight *t*-designs in compact symmetric spaces of rank one. *Proc. Japan Acad.* **61** A(1985), 78–82.
4. E. Bannai and S. G. Hoggar, Tight *t*-designs in projective spaces, and Newton polygons (Proc 10th British Combinatorial Conf., Glasgow 1985). *Ars combinatoria* **20**-A (1985), 43–49.
5. E. Bannai and T. Ito, *Algebraic Combinatorics* II, to appear.
6. A. M. Cohen, Exceptional presentations of three generalised hexagons of order two. Report, Math. Centrum, Amsterdam, 1981.
7. P. Delsarte, J.-M. Goethals and J. J. Seidel, Spherical codes and designs. *Geom. Dedicata* **6** (1977), 363–388.
8. G. Dumas, Sur quelques cas d'irreductibilité des polynomes à coefficients rationnels. *J. Math. Pures et Appl.* **2** (1906), 191–258.
9. P. Erdös, A theorem of Sylvester and Schur. *J. London Math. Soc.* **9** (1934), 282–288.
10. P. Erdös, Note on products of consecutive integers. *J. London Math. Soc.* **14** (1939), 194–198.
11. P. Erdös, On a Diophantine equation. *J. London Math. Soc.* **26** (1951), 176–178.
12. P. Erdös and J. L. Selfridge, The product of consecutive integers is never a power. *Illinois J. Math.* **19** (1975), 292–301.
13. J.-M. Goethals and J. J. Seidel, Cubature formulae, polytopes, and Spherical designs. In *The Geometric Vein (Coxeter Festschrift, Toronto, 1979)*. Springer-Verlag, New York, 1981.

14. O. Hemer, Notes on the Diophantine equation $y^2 - k = x^3$, *Arkiv. Mat.* **3** (1954), 67–77.
15. S. G. Hoggar, t-designs in projective spaces. *Europ. J. Combinatorics* **3** (1982), 233–254.
16. S. G. Hoggar, Tight t-designs and octonians. *Coxeter Festschrift, Teil III*, 1–16 University of Giessen, 1984.
17. S. G. Hoggar, Parameters of t-designs in $\mathbb{F}P^{d-1}$, *Europ. J. Combinatorics* **5** (1984), 29–36.
18. W. Ljunggren, Einige Eigenschaften der Einheiten reeller quadratischer une reinbiquadratischer Zahlkörper, Mit Anwendungen auf die Lösung einer Klasse unbestimmter Gleichungen 4. Grades, *Skr. Norske Vid. Akad. Oslo, Mat.-Naturv. Klasse*, 1936, No. 12, 73 pp.
19. W. Ljunggren, Über die Gleichung $x^4 - Dy^2 = 1$, *Arch. Math. og Naturv.* (*Oslo*) **45** (1942), 61–70.
20. W. Ljunggren, On the Diophantine equation $Ax^4 - By^2 = C\,(C = 1, 4)$, *Math. Scand.* **21** (1967), 149–158.
21. L. J. Mordell, *Diophantine Equations*. Academic Press, 1969.
22. A. Neumaier, Combinatorial configurations in terms of distances. Memorandum 81-09, Eindhoven University of Technology, 1981.
23. I. Niven and H. S. Zuckerman, *An Introduction to the Theory of Numbers*. John Wiley, 1980.
24. H. Rohrbach and J. Weiss, Zum finiten Fall des Bertrandschen Postulats. *J. Reine Angew. Math.* **214/215** (1964), 432–440.
25. J. B. Rosser and L. Schoenfeld, Approximate formulas for some functions of prime numbers. *Illinois J. Math.* **6** (1962), 64–94.
26. G. Szegö, *Orthogonal Polynomials*, 4th edn. American Mathematical Society, Providence, R.I., 1975.

Received 27 February 1986 and in
revised form 10 October 1987

E. BANNAI
Department of Mathematics, Ohio State University,
Columbus, Ohio 43210, U.S.A.
and
S. G. HOGGAR
Department of Mathematics, University of Glasgow,
Glasgow G12 8QW, Scotland