EDITED BY E. F. BECKENBACH, University of California

*Material for this department should be sent directly to E. F. Beckenbach, University of California, Los Angeles 24, California.*

## NEW PROOF OF A MINIMUM PROPERTY OF THE REGULAR $n$-GON

L. F. TOTH, Budapest, Hungary

J. Kurschák gives in his paper *Über dem Kreis ein- und umgeschriebene Vielecke** among others a complete and entirely elementary geometrical proof of the well known fact according to which the regular $n$-gon $\overline{P}_n$ has a minimal area among all $n$-gons $P$ circumscribed about a circle $c$. In this proof $P_n$ is carried, after a dismemberment and a suitable reassembly, in $n-1$ steps into $\overline{P}_n$ so that the area increases at every step.

In this note we give an extremely simple proof,† which appears to be new, showing immediately that if $P_n$ is not regular, then $P_n > \overline{P}_n$, where the area is denoted by the same symbol as the domain.

Consider the circle $C$ circumscribed about $\overline{P}_n$. We show that already for the part $P_n \cdot C$ of $P_n$ lying in $C$ we have

$$P_n \cdot C > \overline{P}_n.$$

We have $P_n \cdot C = C - ns + (s_1s_2 + s_2s_3 + \cdots + s_ns_1)$, where we denote by $s_1, s_2, \cdots, s_n$ the circular sections of $C$ cut off by the consecutive sides of $P_n$, and by $s$ the circular section of $C$ cut off by a tangent to $c$. Hence

$$P_n \cdot C \geqq C - ns.$$

Then

$$P_n \geqq P_n \cdot C \geqq C - ns = \overline{P}_n.$$

Equality holds in $P_n \geqq P_nC$ resp. in $P_nC \geqq \overline{P}_n$ only if no vertex of $P_n$ lies in the outside resp. in the inside of $C$; this completes the proof.

## BINOMIAL COEFFICIENTS MODULO A PRIME

N. J. FINE, University of Pennsylvania

The following theorem, although given by Lucas in his *Theorie des Nombres* (pp. 417–420), does not appear to be as widely known as it deserves to be:

THEOREM 1. *Let $p$ be a prime, and let*

$$M = M_0 + M_1p + M_2p^2 + \cdots + M_kp^k \qquad (0 \leqq M_r < p),$$
$$N = N_0 + N_1p + N_2p^2 + \cdots + N_kp^k \qquad (0 \leqq N_r < p).$$

* Mathematische Annalen 30 (1887), pp. 578–581.

† As P. Szász remarked [Bemerkung zu einer Arbeit von K. Kürschák, Matematikai es Fizikai Lapok XLIV (1937), p. 167, note 3] Kürschák's proof is independent of the axiom of parallels. This advantage is preserved in the present proof.

*Then*

$$\binom{M}{N} \equiv \binom{M_0}{N_0}\binom{M_1}{N_1}\binom{M_2}{N_2}\cdots\binom{M_k}{N_k} \pmod{p}.$$

We offer a short proof of the above theorem:

$$\begin{aligned}\sum_{N=0}^{M}\binom{M}{N}x^N &= (1+x)^M = \prod_{r=0}^{k}\{(1+x)^{p^r}\}^{M_r},\\ &\equiv \prod_{r=0}^{k}(1+x^{p^r})^{M_r} \pmod{p},\\ &= \prod_{r=0}^{k}\left\{\sum_{s_r=0}^{M_r}\binom{M_r}{s_r}x^{s_r p^r}\right\},\\ &= \sum_{N=0}^{M}\left\{\sum\prod_{r=0}^{k}\binom{M_r}{s_r}\right\}x^N,\end{aligned}$$

where the inner sum is taken over all sets $(s_0, s_1, \cdots, s_k)$ such that $\sum_{r=0}^{k} s_r p^r = N$. But $0 \leqq s_r \leqq M_r < p$, so there is at most one such set, given by $s_r = N_r$ $(0 \leqq r \leqq k)$ if every $N_r \leqq M_r$; if not, the sum is zero. The theorem follows by equating coefficients of $x^N$, since

$$\binom{M_r}{N_r} = 0 \quad \text{for} \quad N_r > M_r.$$

THEOREM 2. *Let $T(M)$ be the number of integers $N$ not exceeding $M$ for which*

$$\binom{M}{N} \not\equiv 0 \pmod{p}.$$

*Then*

$$T(M) = \prod_{r=0}^{k}(M_r + 1).$$

Proof: Since $M_r < p$, there are $M_r + 1$ values of $N_r$, given by $0 \leqq N_r \leqq M$, for which

$$\binom{M_r}{N_r} \not\equiv 0 \pmod{p},$$

and these are the only ones.

THEOREM 3. *A necessary and sufficient condition that all the binomial coefficients*

$$\binom{M}{N}, \qquad 0 < N < M,$$

*be divisible by $p$ is that $M$ be a power of $p$.*

Proof: The function $T(M)$ takes the value 2 if and only if one of the $M_r$ is 1 and all the others are 0.

In the opposite direction, we may ask for what values of $M$ *none* of the binomial coefficients

$$\binom{M}{N}, \qquad 0 \leqq N \leqq M,$$

are divisible by $p$.

THEOREM 4. *A necessary and sufficient condition that none of the binomial coefficients of order $M$, with*

$$M = M_0 + M_1 p + \cdots + M_k p^k \qquad (0 \leqq M_r < p;\ M_k > 0)$$

*be divisible by $p$ is that $M_r = p-1$ for $r<k$.*

Proof: Let $M^* = M - M_k p^k$. Suppose first that $T(M) = M+1$. Then

$$\begin{aligned} M_k p^k + M^* + 1 = M + 1 = T(M) &= (M_k + 1)T(M^*) \leqq (M_k + 1)(M^* + 1) \\ &= M_k(M^* + 1) + M^* + 1 \leqq M_k p^k + M^* + 1. \end{aligned}$$

From this chain of inequalities it follows that $M^* = p^k - 1$. Conversely, if $M^* = p^k - 1$, then

$$T(M) = (M_k + 1)p^k = M_k p^k + M^* + 1 = M + 1.$$

Our last theorem deals with the "probability" that a binomial coefficient chosen "at random" will be divisible by $p$. More precisely, consider the $\frac{1}{2}(m+1)(m+2)$ binomial coefficients

$$\binom{M}{N}, \qquad 0 \leqq N \leqq M \leqq m,$$

and let $Q(p;\, m)$ be the fraction of these which are not divisible by $p$.

THEOREM 5. *For every prime $p$,* $\lim_{m\to\infty} Q(p;\, m) = 0$.

Proof: For $k \geqq 0$, let

$$G(k) = \tfrac{1}{2}p^k(p^k + 1)Q(p;\, p^k - 1) = \sum_{M=0}^{p^k-1} T(M).$$

Clearly $G(0) = 1$. Using the notation introduced in the proof of the preceding theorem, we have

$$\begin{aligned} G(k+1) &= \sum_{M=0}^{p^{k+1}-1} T(M) \\ &= \sum_{M_k=0}^{p-1} \sum_{M^*=0}^{p^k-1} (M_k + 1)T(M^*) \end{aligned}$$

$$= \left\{ \sum_{M_k=0}^{p-1} (M_k + 1) \right\} \left\{ \sum_{M^*=0}^{p^k-1} T(M^*) \right\}$$
$$= \tfrac{1}{2} p(p+1) G(k).$$

It follows immediately that $G(k) = (\frac{1}{2}p(p+1))^k$. Now suppose that $p^k \leqq m < p^{k+1}$. Then

$$Q(p; m) \leqq \frac{2}{(m+1)(m+2)} G(k+1) < 2p^{-2k} G(k+1) = 2p^{-2k}(\tfrac{1}{2}p(p+1))^{k+1}$$
$$= p(p+1)\left(\frac{1+1/p}{2}\right)^k,$$

which tends to 0 with increasing $m$.

By an obvious extension it follows that, given an arbitrary finite set of primes, it is "virtually certain" that a binomial coefficient chosen at random will be divisible by all the primes in the set.

## VOLUME OF AN $n$-DIMENSIONAL SPHERE

H. P. EVANS, University of Wisconsin

1. **Introduction.** That certain definite integrals may be evaluated from probability considerations is well known [1]. It will be shown that the evaluation of the multiple integral for the volume of an $n$-dimensional sphere may be obtained from the probability distribution of the sum of squares of $n$ independent and normally distributed random variables, all having the same standard deviation $\sigma$ and mean zero. Since the study of this distribution is a standard topic for courses in both probability theory [1] and mathematical statistics [2, 3, 4], and since the formula for the volume of an $n$-dimensional sphere is derivable by the methods of advanced calculus [5, 6], a consequence of the present note is the establishment of a further connection between the methods of probability theory and the methods of advanced calculus.

2. **Analytical development.** Let $x_i$ $(i=1, 2, \cdots, n)$ be $n$ independent and normally distributed random variables, each having the standard deviation $\sigma$ and the mean value zero. If we put $x = \sum x_i^2$, where the summation is from 1 to $n$, it is known from probability theory that the probability density function for $x$ is

$$\text{(1)} \qquad \begin{cases} f(x) = \dfrac{(2\sigma^2)^{-n/2}}{\Gamma\left(\dfrac{n}{2}\right)} x^{n/2-1} e^{-x/2\sigma}, & x > 0, \\ f(x) = 0, & x \leqq 0. \end{cases}$$

From the given distribution of the $x_i$'s it follows that the distribution function for $x = \sum x_i^2$ is