$a \pmod p \leqslant b \pmod p$ for All Primes p Implies $a = b$

P. ERDŐS
Mathematical Institute of the Hungarian Academy of Sciences, Budapest, Hungary

P. P. PÁLFY
Mathematical Institute of the Hungarian Academy of Sciences, Budapest, Hungary

M. SZEGEDY
Eötvös University, Budapest, Hungary

The reader might wonder about the abundance of authors for such a short note. The assertion of the title was conjectured by P. P. Pálfy, and P. Erdős pointed out that it easily follows from the Sylvester-Schur theorem. Then it was set as a problem in the 1984 Hungarian annual M. Schweitzer memorial mathematics contest for college students. The most elegant solution was given by M. Szegedy, and that is what we present here.

THEOREM. *Let a and b be positive integers. If, divided by any prime number, the residue of a is less than or equal to the residue of b, then a and b are equal.*

Proof. Let us use the notation x_p for the residue of x modulo p, i.e., $x \equiv x_p \pmod p$ and $0 \leqslant x_p < p$. If we choose $p > \max(a, b)$, then $a = a_p \leqslant b_p = b$. We will suppose $a < b$ and prove the theorem by contradiction.

We have $1 \leqslant b - a < b$ and $(b - a)_p = b_p - a_p \leqslant b_p$, so $b - a$ and b satisfy the hypothesis of the theorem if and only if a and b do. So, without loss of generality, we may choose the smaller of a and $b - a$, call it a and have $1 \leqslant a \leqslant b/2$.

We can reach a contradiction immediately by making use of the Sylvester-Schur theorem [1]. It yields a prime $p > a$ such that p divides $\binom{b}{a}$, i.e., $p \mid (b - a + 1) \cdots (b - 1)b$. Exactly one of the factors will be divisible by p, say $b - k$, $0 \leqslant k < a$. But then $b_p = k < a = a_p$, contrary to the assumption.

However, we can give a more elementary, self-contained proof. Let

$$A = 1 \cdot 2 \cdots (a - 1)a \quad \text{and} \quad B = (b - a + 1) \cdots (b - 1)b,$$

so that $B/A = \binom{b}{a}$. Let $\alpha(p^k)$ and $\beta(p^k)$ be the number of factors in A and B, respectively, which are divisible by p^k. Thus

$$A = \prod_p p^{\sum_{k=1}^{\infty} \alpha(p^k)}, \quad B = \prod_p p^{\sum_{k=1}^{\infty} \beta(p^k)}.$$

Since both A and B are products of a consecutive integers and multiples of p^k appear p^k integers apart in the sequence of integers, we have

$$\left|\alpha(p^k) - \beta(p^k)\right| \leqslant 1.$$

By hypothesis, $a_p \leqslant b_p$. That is, the first multiple of p in the sequence $a, a-1, \ldots, 1$ will occur not later than the first multiple of p in the sequence $b, b-1, \ldots, b-a+1$. Thus $\alpha(p) \geqslant \beta(p)$. But if $p > a$, then $\alpha(p) = 0$. So, $\beta(p) = 0$ also, and neither A nor B is divisible by p.

We have

$$\binom{b}{a} = \frac{B}{A} = \prod_{p \leqslant a} p^{\sum_{k=1}^{\infty} \beta(p^k) - \sum_{k=1}^{\infty} \alpha(p^k)}.$$

Denoting by $\kappa(p)$ the exponent of the highest power of p for which $\beta(p^k) > 0$ we get

$$\sum_{k=1}^{\infty} (\beta(p^k) - \alpha(p^k)) = \beta(p) - \alpha(p) + \sum_{k=2}^{\kappa(p)} (\beta(p^k) - \alpha(p^k)) - \sum_{k=\kappa(p)+1}^{\infty} \alpha(p^k) \leqslant \sum_{k=2}^{\kappa(p)} 1 = \kappa(p) - 1.$$

Therefore

$$\frac{B}{A} \Bigg| \prod_{p \leqslant a} p^{\kappa(p)-1},$$

or put in another way

$$\frac{(b-a+1)\cdots(b-1)b}{\prod_{p \leqslant a} p^{\kappa(p)}} \Bigg| \frac{1 \cdot 2 \cdots (a-1)a}{\prod_{p \leqslant a} p}.$$

Here, after factoring, there remain in the right-hand side exactly $a - \pi(a)$ factors each at most a, and in the left-hand side at least $a - \pi(a)$ such factors which are $\geqslant b - a + 1$. Since $b \geqslant 2a$, $b - a + 1 \geqslant a + 1 > a$, so we have a contradiction.

REFERENCE

1. P. Erdős, A Theorem of Sylvester and Schur, J. London Math. Soc., 9 (1934) 282–288.

THE TEACHING OF MATHEMATICS

EDITED BY JOAN P. HUTCHINSON AND STAN WAGON

The Classification of 1-Manifolds: A Take-Home Exam

DAVID GALE
Department of Mathematics, University of California, Berkeley, CA 94720

1. Introduction. An effective and much used method for introducing students to a new mathematical topic (e.g., modern algebra) is to pick some important subtopic (say, groups) and then present a discussion of the simplest or most familiar special