



---

On a Congruence modulo a Prime

Author(s): Hao Pan

Source: *The American Mathematical Monthly*, Vol. 113, No. 7 (Aug. - Sep., 2006), pp. 652-654

Published by: Mathematical Association of America

Stable URL: <http://www.jstor.org/stable/27642010>

Accessed: 24/03/2010 21:35

---

Your use of the JSTOR archive indicates your acceptance of JSTOR's Terms and Conditions of Use, available at <http://www.jstor.org/page/info/about/policies/terms.jsp>. JSTOR's Terms and Conditions of Use provides, in part, that unless you have obtained prior permission, you may not download an entire issue of a journal or multiple copies of articles, and you may use content in the JSTOR archive only for your personal, non-commercial use.

Please contact the publisher regarding any further use of this work. Publisher contact information may be obtained at <http://www.jstor.org/action/showPublisher?publisherCode=maa>.

Each copy of any part of a JSTOR transmission must contain the same copyright notice that appears on the screen or printed page of such transmission.

JSTOR is a not-for-profit service that helps scholars, researchers, and students discover, use, and build upon a wide range of content in a trusted digital archive. We use information technology and tools to increase productivity and facilitate new forms of scholarship. For more information about JSTOR, please contact [support@jstor.org](mailto:support@jstor.org).



*Mathematical Association of America* is collaborating with JSTOR to digitize, preserve and extend access to *The American Mathematical Monthly*.

<http://www.jstor.org>

# On a Congruence modulo a Prime

Hao Pan

In 1961, Erdős, Ginzburg, and Ziv [3] proposed the following celebrated theorem, which is now known as the origin of zero-sum problems. (For the further developments of zero-sum problems, the reader can refer to [1], [2], and [5].)

**The EGZ Theorem.** *Suppose that  $n$  is a positive integer. Then for any sequence  $a_1, \dots, a_{2n-1}$  of  $2n - 1$  integers there exists a subsequence  $a_{i_1}, \dots, a_{i_n}$  of length  $n$  such that the sum  $\sum_{j=1}^n a_{i_j}$  is divisible by  $n$ .*

It is easy to check that the EGZ theorem is multiplicative, that is, if the statement holds for both  $n = k$  and  $n = l$ , then it also holds for  $n = kl$ . Thus it is sufficient to prove the EGZ theorem when  $n$  is a prime.

In the classical proofs of the theorem, the case where  $n$  is a prime is usually deduced from the Cauchy-Davenport theorem or the Chevalley-Waring theorem (see [6]). However, with the help of a Vandermonde determinant, Gao [4] gave another proof of the EGZ theorem based on the following congruence:

$$\sum_{\substack{I \subseteq \{1, \dots, 2p-1\} \\ |I|=p}} \left( \sum_{i \in I} a_i \right)^{p-1} \equiv 0 \pmod{p}, \tag{*}$$

where  $p$  is a prime and  $a_1, \dots, a_{2p-1}$  are arbitrary integers. Note that the EGZ theorem is an immediate consequence of (\*), since by Fermat's little theorem we have

$$\begin{aligned} & \left| \left\{ I \subseteq \{1, \dots, 2p-1\} : \sum_{i \in I} a_i \equiv 0 \pmod{p} \text{ \& } |I| = p \right\} \right| \\ & \equiv \sum_{\substack{I \subseteq \{1, \dots, 2p-1\} \\ |I|=p}} \left( 1 - \left( \sum_{i \in I} a_i \right)^{p-1} \right) \equiv \binom{2p-1}{p} \equiv 1 \pmod{p}. \end{aligned}$$

In this paper, we establish the following theorem, which clearly implies Gao's congruence:

**Theorem.** *Suppose that  $p$  is a prime and that  $k$  is a positive integer with  $k \leq p$ . Let  $f(x_1, \dots, x_k)$  be a symmetric polynomial with integral coefficients in the variables  $x_1, \dots, x_k$ . If the degree of  $f$  is less than  $k$ , then for an arbitrary sequence of  $p + k - 1$  integers  $a_1, \dots, a_{p+k-1}$  it is true that*

$$\sum_{1 \leq i_1 < \dots < i_k \leq p+k-1} f(a_{i_1}, \dots, a_{i_k}) \equiv \begin{cases} f(0, \dots, 0) \pmod{p} & \text{if } k = p, \\ 0 \pmod{p} & \text{otherwise.} \end{cases}$$

*Proof.* The proof is elementary, requiring only a basic arithmetic property of binomial coefficients:

$$\binom{p+k-1}{k} = \frac{p(p+1) \cdots (p+k-1)}{k!} \equiv \begin{cases} 1 \pmod{p} & \text{if } k = p, \\ 0 \pmod{p} & \text{if } 1 \leq k < p. \end{cases}$$

We argue by an induction on  $k$ . When  $k = 1$ , since  $\deg f < k$ ,  $f$  must be a constant  $c$ . In this case  $\sum_{1 \leq i \leq p} f(a_i) = pc \equiv 0 \pmod{p}$ . Now assume that  $k > 1$  and that the theorem holds for all smaller values of  $k$ .

Let

$$S_{f,k}(x_1, \dots, x_{p+k-1}) = \sum_{1 \leq i_1 < \dots < i_k \leq p+k-1} f(x_{i_1}, \dots, x_{i_k}),$$

and write  $f(x_1, \dots, x_k)$  in the form

$$f(x_1, \dots, x_k) = \sum_{j=0}^{k-1} g_j(x_1, \dots, x_{k-1})x_k^j,$$

where the  $g_j$  are polynomials in the variables  $x_1, \dots, x_{k-1}$ . From the symmetry of  $f$  it follows that  $S_{f,k}$  and all the  $g_j$  are likewise symmetric polynomials. Next observe that

$$S_{f,k}(a_1, \dots, a_{p+k-1}) = \sum_{1 \leq i_1 < \dots < i_k \leq p+k-2} f(a_{i_1}, \dots, a_{i_k}) + \sum_{1 \leq i_1 < \dots < i_{k-1} \leq p+k-2} f(a_{i_1}, \dots, a_{i_{k-1}}, a_{p+k-1}).$$

Thus

$$\begin{aligned} & S_{f,k}(a_1, \dots, a_{p+k-2}, a_{p+k-1}) - S_{f,k}(a_1, \dots, a_{p+k-2}, 0) \\ &= \sum_{1 \leq i_1 < \dots < i_{k-1} \leq p+k-2} (f(a_{i_1}, \dots, a_{i_{k-1}}, a_{p+k-1}) - f(a_{i_1}, \dots, a_{i_{k-1}}, 0)) \\ &= \sum_{1 \leq i_1 < \dots < i_{k-1} \leq p+k-2} \left( \sum_{j=0}^{k-1} g_j(a_{i_1}, \dots, a_{i_{k-1}}) a_{p+k-1}^j - g_0(a_{i_1}, \dots, a_{i_{k-1}}) \right) \\ &= \sum_{j=1}^{k-1} a_{p+k-1}^j \sum_{1 \leq i_1 < \dots < i_{k-1} \leq p+k-2} g_j(a_{i_1}, \dots, a_{i_{k-1}}) \\ &= \sum_{j=1}^{k-1} a_{p+k-1}^j S_{g_j, k-1}(a_1, \dots, a_{p+k-2}). \end{aligned}$$

Since  $k \leq p$  and  $\deg g_j \leq \deg f - j < k - j$ , we can invoke the induction hypothesis to conclude that for  $j = 1, 2, \dots, k - 1$

$$S_{g_j, k-1}(a_1, \dots, a_{p+k-2}) \equiv 0 \pmod{p}.$$

Therefore

$$S_{f,k}(a_1, \dots, a_{p+k-2}, a_{p+k-1}) \equiv S_{f,k}(a_1, \dots, a_{p+k-2}, 0) \pmod{p}.$$

In light of the symmetry of  $S_{f,k}$ , we have

$$S_{f,k}(a_1, \dots, a_{p+k-1}) \equiv S_{f,k}(0, \dots, 0) \pmod{p}.$$

Finally, from the definition of  $S_{f,k}$  we conclude that

$$\begin{aligned} S_{f,k}(0, \dots, 0) &= \binom{p+k-1}{k} f(0, \dots, 0) \\ &\equiv \begin{cases} f(0, \dots, 0) & (\text{mod } p) \text{ if } k = p, \\ 0 & (\text{mod } p) \text{ if } 1 \leq k < p. \end{cases} \end{aligned}$$

This concludes the proof. ■

#### REFERENCES

---

1. N. Alon and M. Dubiner, Zero-sum sets of prescribed size, in *Combinatorics, Paul Erdős is Eighty*, vol. 1, János Bolyai Math. Soc., Budapest, 1993, pp. 33–50.
2. Y. Caro, Zero-sum problems—A survey, *Discrete Math.* **152** (1996) 93–113.
3. P. Erdős, A. Ginzburg, and A. Ziv, Theorem in the additive number theory, *Bull. Research Council Israel* **10F** (1961) 41–43.
4. W. D. Gao, Two addition theorems on groups of prime order, *J. Number Theory* **56** (1996) 211–213.
5. W. D. Gao and A. Geroldinger, On zero-sum sequences in  $\mathbb{Z}/n\mathbb{Z} \oplus \mathbb{Z}/n\mathbb{Z}$ , *Integers* **3** (2003) A8 (electronic).
6. M. B. Nathanson, *Additive Number Theory: Inverse Problems and the Geometry of Sumsets*, Springer-Verlag, New York, 1996.

*Department of Mathematics, Nanjing University, Nanjing 210093, People's Republic of China*  
*haopan79@yahoo.com.cn*