A NOTE ON STEPHAN'S CONJECTURE 25

ELIZABETH WILMER AND OLIVER SCHIROKAUER

Recently Stephan [3] posted 117 conjectures based on an extensive analysis of the On-line Encyclopedia of Integer Sequences [1, 2]. Here we give an entirely elementary proof of a generalization of Conjecture 25.

As usual, we write $\phi(n)$ for the order of $(\mathbb{Z}/n\mathbb{Z})^*$, the multiplicative group of invertible elements modulo n.

Fix a prime $p > 1$ and a positive integer $k > 1$. For all non-negative integers n, let $C(n)$ be the number of distinct k-th powers, modulo p^{kn}.

Lemma 1. *If $p^{k(n-1)}|(a-b)$, then $p^{kn}|((pa)^k - (pb)^k)$.*

Proof. Observe that

$$(pa)^k - (pb)^k = p^k(a-b)(a^{k-1} + a^{k-2}b + \cdots + b^{k-1})$$

and apply the hypothesis to the second factor. □

Lemma 2. *When k is relatively prime to both p and $p-1$,*

$$C(n) = (p-1)p^{kn-1} + C(n-1) \quad \textit{for all } n \geq 1.$$

Proof of Lemma. First note that

$$\left|\left(\mathbb{Z}/p^{kn}\mathbb{Z}\right)^*\right| = \phi(p^{kn}) = (p-1)p^{kn-1}.$$

Since k is relatively prime to both p and $p-1$, the homomorphism from the abelian group $\left(\mathbb{Z}/p^{kn}\mathbb{Z}\right)^*$ to itself given by raising each element to the k-th power is injective. Thus, the k-th powers of the invertible remainders are all distinct and contribute $\phi(p^{kn})$ to the residue count.

What about the non-invertible remainders? Since p is prime, every non-invertible remainder is a multiple of p. By Lemma 1,

$$p(0), p(1), p(2), \ldots, p(p^{k(n-1)} - 1)$$

will together generate all distinct non-invertible k-th powers, modulo p^{kn}. Since

$$p^{kn} \left| \left((pa)^k - (pb)^k\right) \quad \text{iff} \quad p^{k(n-1)} \right| \left(a^k - b^k\right),$$

together these values will contribute exactly $C(n-1)$ distinct k-th powers, modulo p^{kn}. □

Date: October 15, 2004.

Proposition 3. *When k is relatively prime to both p and $p-1$ and $n \geq 0$,*

$$C(n) = (p-1)p^{k-1}\left(\frac{p^{kn}-1}{p^k-1}\right) + 1.$$

Proof. First note that $C(0) = 1$. By Lemma 2, when $n \geq 1$ we have

$$\begin{aligned} C(n) &= (p-1)p^{kn-1} + (p-1)p^{k(n-1)-1} + \cdots + (p-1)p^{k-1} + 1 \\ &= (p-1)p^{k-1}\left(p^{k(n-1)} + \cdots + p^{k(0)}\right) + 1 \\ &= (p-1)p^{k-1}\left(\frac{p^{kn}-1}{p^k-1}\right) + 1. \end{aligned}$$

(In the last step, we merely summed the geometric series.) □

Corollary 4 (Conjecture 25)**.** *For all non-negative integers n, there are*

$$\frac{4(8^n)+3}{7}$$

cubic residues modulo 8^n.

Proof. Set $p = 2$ and $k = 3$. □

References

[1] Sloane, N. J. A. The On-Line Encyclopedia of Integer Sequences, published electronically at `http://www.research.att.com/ñjas/sequences/`, 2004.

[2] Sloane, N. J. A. The on-line encyclopedia of integer sequences. *Notices Amer. Math. Soc.* **50** (2003), pp. 912–915.

[3] Stephan, Ralf. Prove or Disprove: 100 Conjectures from the OEIS. arXiv:math.CO/0409509

Department of Mathematics, Oberlin College, Oberlin, OH 44074
E-mail address: `elizabeth.wilmer@oberlin.edu`