On the parity of k-th powers modulo p

Jennifer Paulhus

Kansas State University
paulhus@math.ksu.edu
www.math.ksu.edu/∼paulhus

This is joint work with Todd Cochrane and Chris Pinner of Kansas State University and Jean Bourgain of the Institute for Advanced Study.

Notation

p will denote an odd prime
$\mathbb{O} = \{1, 3, 5, \ldots, p-2\} \subset \mathbb{Z}/p\mathbb{Z}$ the odd residues
$\mathbb{E} = \{2, 4, 6, \ldots, p-1\} \subset \mathbb{Z}/p\mathbb{Z}$ the even residues
$e_p(*) = e^{2\pi i */p}$

We consider

$$N_k = N_k(A) = \#\{x \in \mathbb{E} \mid Ax^k \in \mathbb{O}\}$$

where k and A are any integers with $p \nmid A$.

In previous work, we showed $N_k > 0$ for p sufficiently large and $(k, p-1) = 1$, resolving a conjecture of Goresky and Klapper.

A Generalization

Lehmer posed the problem of determining $N_{-1}(1)$, the number of even residues with odd multiplicative inverse (mod p). The expectation is that $N_{-1}(1) \sim p/4$, which was later proven by Zhang.

For example when $p = 13$, $N_{-1}(1) = 3$.

Residue	Inverse	Residue	Inverse
2	7	8	5
4	10	10	4
6	11	12	12

In the general setting we no longer always have $N_k \sim p/4$.

k even

$$\Phi(k) = \max_{\substack{a \in \mathbb{Z}/p\mathbb{Z} \\ a \neq 0}} \left| \sum_{x \neq 0} e_p(ax^k) \right|, \quad \Phi'(k) = \max_{\substack{a \in \mathbb{Z}/p\mathbb{Z} \\ a \neq 0}} \left| \sum_{x=1}^{(p-1)/2} e_p(ax^k) \right|$$

When k is even, $\Phi'(k) = \frac{1}{2}\Phi(k)$.

Theorem

For any integer k

$$\left| N_k - \frac{p}{4} \right| < \frac{1}{\pi} \Phi'(k) \min\{\log\left(\frac{356p}{\Phi'(k)}\right), \log(5p)\}$$

When $\Phi(k) = o(p)$ then $N_k \sim p/4$.

k odd

Two parameters which help dictate the bias are $d = (k, p-1)$ and $d_1 = (k-1, p-1)$.
Similarly we have the values $s = \frac{p-1}{d}$ and $t = \frac{p-1}{d_1}$.

Theorem

(a) If k is odd and t is even then

$$\left|N_k - \frac{p}{4}\right| \leq 0.35 p^{89/92} \log^{3/2}(5p)$$

(b) If k is odd and t is odd then

$$\left|N_k - \frac{p}{4}\right| \ll d_1 + \frac{p}{\log p}$$

As long as $d_1 = o(p)$ then $N_k \sim p/4$.

Small $s = \frac{p-1}{d}$

An Example

If $k = p - 1$, $x^k = 1$ identically so $N_k = 0$ or $\frac{p-1}{2}$ depending on whether A is even or odd.

If $k = \frac{p-1}{2}$, $x^k = \pm 1$. A and $-A$ have opposite parity and roughly half even residues are quadratic residues so $N_k \sim \frac{p}{4}$.

If $k = \frac{p-1}{3}$ then $Ax^k \equiv AC_1, AC_2,$ or $AC_3 \bmod p$ where the C_i are the cube roots of unity. Then $N_k = 0, \frac{p-1}{6}, \frac{p-1}{3}$, or $\frac{p-1}{2}$ depending on how many AC_i are odd.

Small $s = \frac{p-1}{d}$, continued

These examples suggest the following theorem.

Theorem

Let k, A be any integers with $p \nmid A$ and $(\mathbb{Z}/p\mathbb{Z}^*)^k = \{C_1, \ldots, C_s\}$.

(a) If k is even then $N_k = \frac{p-1}{2s} \sum_{i=1}^{s} \chi_{\mathbb{O}}(AC_i)$. In particular if k is even and s is even then $N_k = \frac{p-1}{4}$.

(b) If k is odd then $\left| N_k - \frac{p-1}{4} \right| < \frac{s-1}{2\pi} \sqrt{p} \log(5p)$.

For a set I, $\chi_I(x)$ is the characteristic function, which is 1 if $x \in I$ and zero otherwise.

Small $t = \frac{p-1}{d_1}$

An Example

If $k = \frac{p+1}{2}$ then $t = 2$ and $Ax^k \equiv Ax$ or $-Ax \bmod p$ depending on whether x is a quadratic residue or not. So we expect about half the even residues to become odd.

If $k = \frac{p+2}{3}$ then $t = 3$ and $Ax^k \equiv AC_1x, AC_2x$ or $AC_3x \bmod p$

To compute N_k in this example we need to study the distribution of points on the lattices $y \equiv AC_ix \bmod p$.

When none of the lattices have a small nonzero point then even and odd values are equidistributed and $N_k \sim \frac{p}{4}$.

Bias

If one of the lattices has a small point, there may be bias.

An Example

If $k = \frac{p+2}{3}$ *then* $t = 3$ *and* $Ax^k \equiv AC_1x, AC_2x$ *or* $AC_3x \bmod p$. *Our results give that, depending on the size of the smallest point in the lattices,* N_k *is asymptotically between* $\frac{p}{4} - \frac{p}{12}$ *and* $\frac{p}{4} + \frac{p}{12}$.

Another Example

When t *and* $|A|$ *are both small odd numbers we get bias. In particular if* $|A| < (p/t)^{1/2(t-1)}$ *and* $t \ll \log p$ *then*

$$N_k \sim \left(1 - \frac{1}{At}\right)\frac{p}{4}$$

The End