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 $N_k \sim p/4$.

A general estimate for N_k

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

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 k is even, $\Phi'(k) = \frac{1}{2}\Phi(k)$ and so $N_k \sim p/4$ when $\Phi(k) = o(p)$.

Ideas of Proof

Let $S = \{x_n\}$ be a sequence defined by $x_n \equiv A2^{k-1}n^k \bmod p$ for $1 \leq n \leq \frac{p-1}{2}$ and $I = \{-1, -2, \ldots, -\frac{p-1}{2}\}$.

$x_n \in I$ precisely when $A(2n)^k \in \mathbb{O}$ so $N_k = \sum_{n=1}^{\frac{p-1}{2}} \chi_I(x_n)$.

Using the Fourier expansion of χ_I and bounds on exponential sums we obtain the second estimate in the theorem: $|N_k - p/4| < \frac{1}{\pi}\Phi'(k)\log(5p)$.

A better bound is obtained by using a smooth approximation to the characteristic function which leads to an Erdös-Turán type inequality.

Ideas of Proof, continued

Theorem

For any sequence $S = (x_1, \ldots, x_N) \in \mathbb{Z}/p\mathbb{Z}$, interval $I = \{a+1, a+2, \ldots, a+M\} \subset \mathbb{Z}/p\mathbb{Z}$, and positive $H < p$

$$\left| \sum_{n=1}^{N} \chi_I(x_n) - \frac{MN}{p} \right| \leq \frac{N}{H+1} - \frac{N}{p} + \frac{2}{\pi}\left(\log H + \gamma + \frac{\pi}{2}\right)\Phi_S$$

where γ is Euler's constant and

$$\Phi_S = \max_{p \nmid y} \left| \sum_{n=1}^{N} e_p(yx_n) \right|.$$

The left hand side corresponds to measuring the discrepancy of the sequence of points x_n/p mod 1.

To obtain the constants here we use a bound of Vaaler on the discrepancy of a sequence. The bound can be improved since our interval is of length $\frac{1}{2}$.

Restating

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

Theorem

For any integer k

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

k odd

Two parameters which help dictate the bias in the parity of kth powers 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 $\left| N_k - \frac{p-1}{4} \right| < \frac{s-1}{2\pi} \sqrt{p} \log(5p)$.

Ideas of Proof

Again, let $\{C_1, \ldots, C_s\}$ be the kth powers in $\mathbb{Z}/p\mathbb{Z}^*$ and define c_i such that $c_i^k \equiv C_i \bmod p$.

$$N_k = \sum_x \chi_{\mathbb{E}}(x)\chi_{\mathbb{O}}(Ax^k) = Main + Error$$

where, after some manipulations,

$$Main = \frac{p-1}{2s} \sum_{i=1}^{s} \chi_{\mathbb{O}}(AC_i)$$

$$Error = \frac{1}{s} \sum_{\substack{\psi^s = \psi_0 \\ \psi \neq \psi_0}} \sum_{i=1}^{s} \chi_{\mathbb{O}}(AC_i)\psi(\overline{c_i}) \sum_{x \neq 0} \psi(x)\chi_{\mathbb{E}}(x)$$

Ideas of Proof, continued

If $\psi(-1) = 1$ then $\sum_{x=1}^{\frac{p-1}{2}} \psi(x) = \frac{1}{2}\sum_x \psi(x) = 0$. This will happen to all ψ satisfying $\psi^s = \psi_0$ if k is even. Hence $Error = 0$.

If $\psi(-1) = -1$ we need to use a bound of Polya, Landau, Schur, and Vinogradov for incomplete character sums.

$$\left|\sum_x \psi(x)\chi_{\mathbb{E}}(x)\right| = \left|\sum_{x=1}^{(p-1)/2} \psi(x)\right| \le \frac{1}{\pi}\sqrt{p}\log(5p).$$

When k is odd exactly half the ψ satisfying $\psi^s = \psi_0$ will also satisfy $\psi(-1) = -1$.

$$|Error| < \frac{s-1}{2\pi}\sqrt{p}\log(5p).$$

Restating

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 $\left| N_k - \frac{p-1}{4} \right| < \frac{s-1}{2\pi} \sqrt{p} \log(5p)$.

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*

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

Open Problems

How large does s need to be for $\Phi(k) = o(p)$?

- Work of Bourgain says there is a constant c such that $\Phi(k) = o(p)$ if $s > p^{\frac{c}{\log\log p}}$.
- Montgomery, Vaughan, and Wooley conjecture $\Phi(k) \ll \sqrt{dp\log p}$ which would give $\Phi(k) = o(p)$ if $\frac{\log p}{s} \to 0$ as $p \to \infty$.
- We know from Shparlinski that $\Phi(k) = o(p)$ requires $\frac{s}{\log p} \to \infty$ as $p \to \infty$.

When is $N_k = 0$?

- If $p = \frac{3^s - 1}{2}$ and $k = \frac{p-1}{s}$ then the k-th powers are just $<3> = \{1, 3, 3^2, \ldots, 3^{s-1}\}$ which are all odd.
- Here $s \approx \log p$, are there examples with larger s?

The End