Statistics for fixed points of $x \mapsto x^x \bmod p$

ROSE-HULMAN INSTITUTE OF TECHNOLOGY

Matthew Friedrichsen and Joshua Holden

Forging a (variant) ElGamal Digital Signature

Frank the Forger wants to solve for r and s in:

(1) $$g^{H(m)} \equiv y^s r^r \pmod{p}.$$

He knows m, g, y, and p but not the discrete log of y mod p base g. He could:

- calculate the discrete log of y,
- or he could solve $r^r \equiv g^{H(m)} y^{-s} \pmod{p}$ for r.

We wish to shed light on the difficulty of the second attack by studying the *self-power map*, $x \mapsto x^x \bmod p$.

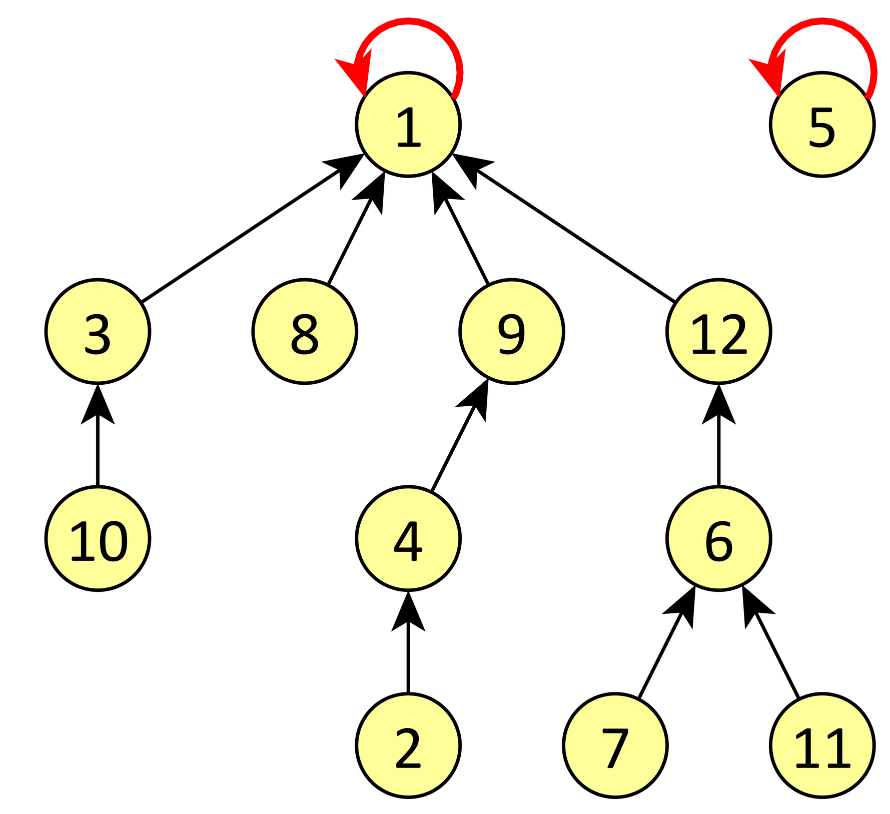

Figure 1: The self-power map modulo 13

Is $x \mapsto x^x \bmod p$ "random"?

Heuristic 1. *For all p, if x, y are chosen uniformly at random from $\{1, \ldots, p-1\}$ with $\operatorname{ord}_p x = d$, then*

$$\Pr[x^x \equiv y \pmod{p}] \approx \begin{cases} \frac{1}{d} & \text{if } \operatorname{ord}_p y \mid d, \\ 0 & \text{otherwise.} \end{cases}$$

Counts of the fixed points are not normally distributed

This work investigates the number of *fixed points* of the self-power map, i.e., solutions to

(2) $$x^x \equiv x \pmod{p}.$$

Let $F(p)$ be the number of solutions to (2) such that $1 \le x \le p-1$. How are these counts distributed? The figures show that the distribution is not (quite) normal.

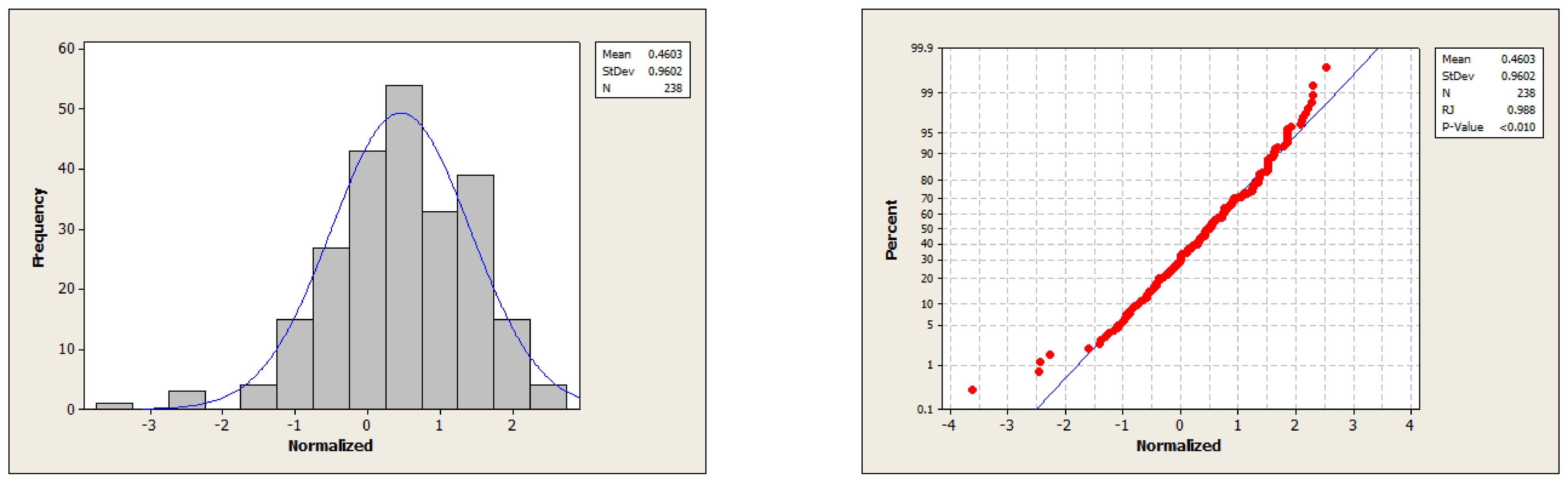

Figure 2: Histogram and Probability Plot of z-statistics for 238 six-digit primes

The counts for most orders are binomially distributed

Let $F_d(p)$ be the number of solutions to (2) with $1 \le x \le p-1$ and $\operatorname{ord}_p x = d$. Assume x values behave independently.

Prediction 2.

$$\Pr[F_d(p) = k] = \binom{\phi(d)}{k} \left(\frac{1}{d}\right)^k \left(\frac{d-1}{d}\right)^{\phi(d)-k}$$

A chi-squared goodness-of-fit test gives

$$p\text{-value} \approx 0.198$$

which does not refute the prediction.

We also tried a sliding window chi-squared test on the data sorted by order. The resulting p-values should be uniformly distributed but are not for small and large d.

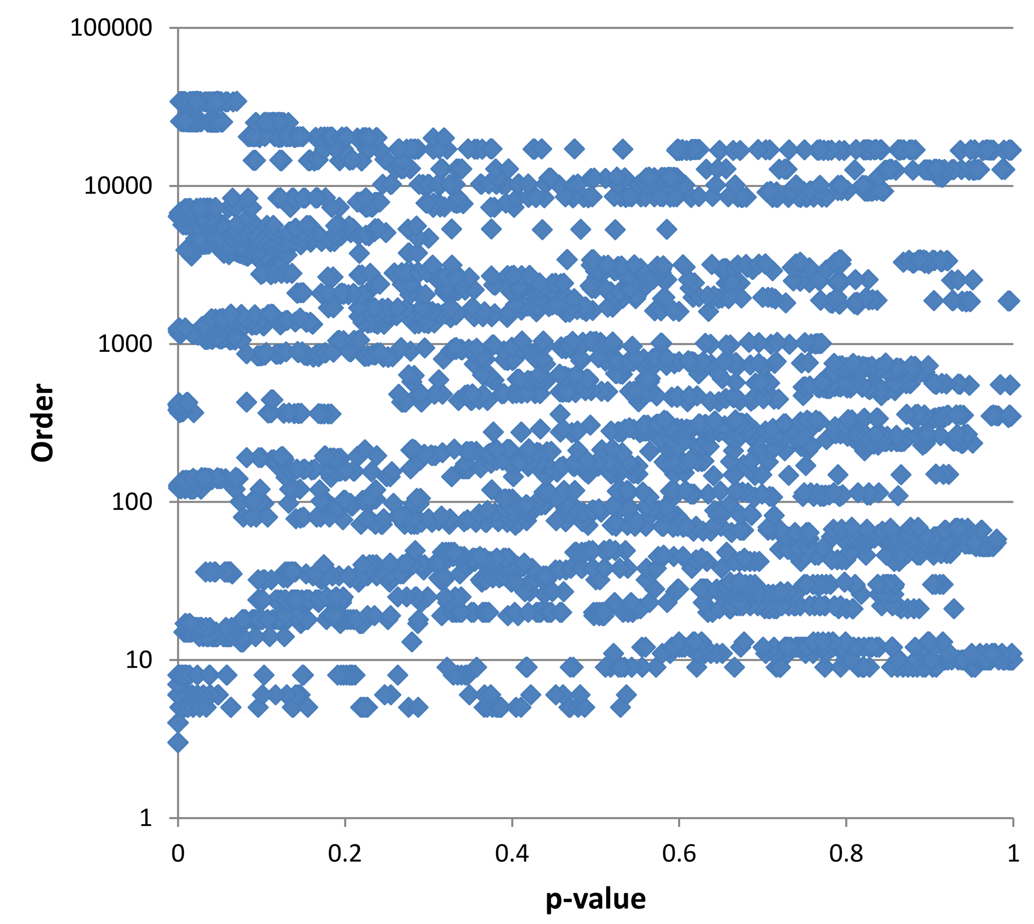

Figure 3: Logarithmic plot showing p-values of the sliding window test for 238 six-digit primes

Dependencies matter for small and large orders

For small and large orders it turns out that the independence assumption is violated.

Theorem 3.
(a) *The x-values of order 3 cannot both be fixed points.*
(b) *The x-values of order 4 cannot both be fixed points.*
(c) *The x-values of order 6 are both fixed points or neither is.*

There are similar effects for $d = (p-1)/3$ and $d = (p-1)/4$, and possibly a few others.

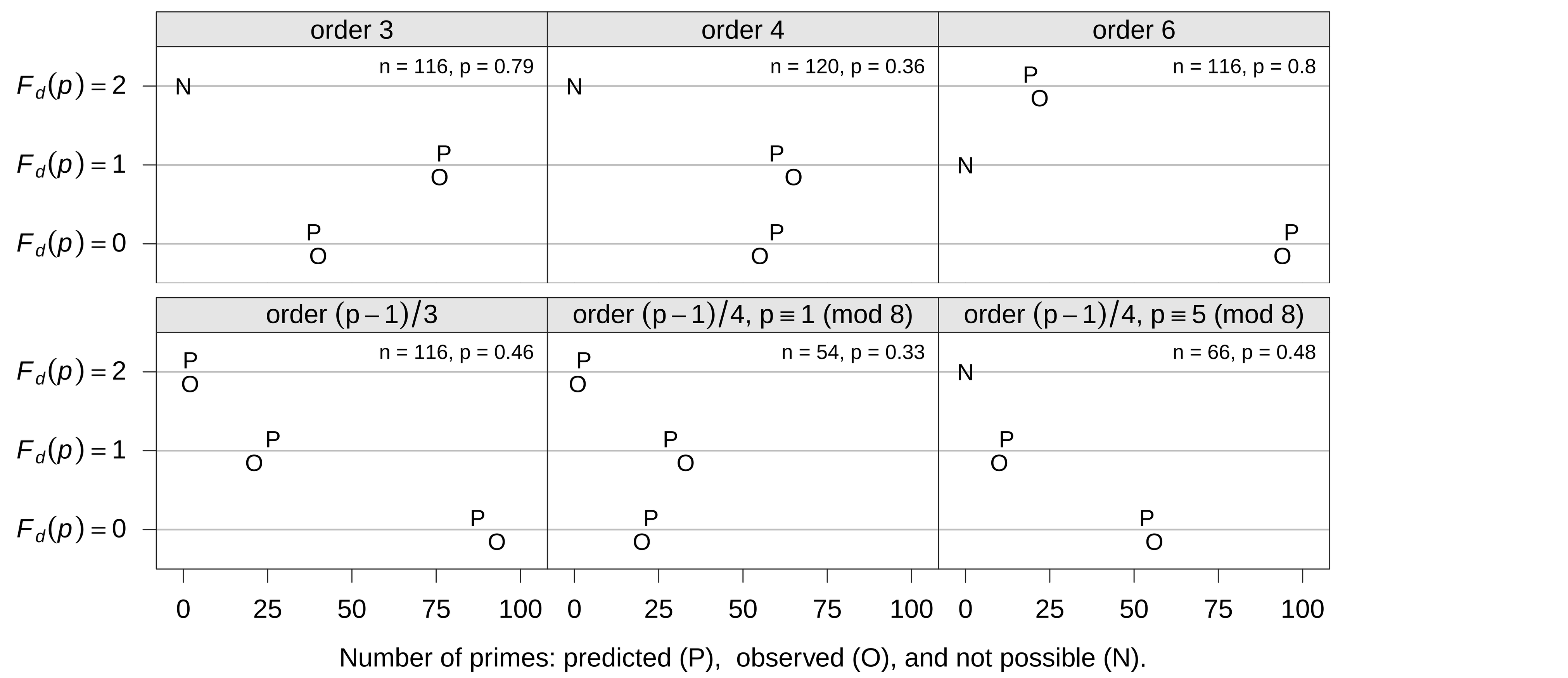

Figure 4: Predictions and observations for fixed points of small and large orders in 238 six-digit primes

Our predictions based on these dependencies are not refuted by chi-squared tests.