Fixed points and 2-cycles of $x \mapsto x^x$ mod n

Joshua Holden

ROSE-HULMAN INSTITUTE OF TECHNOLOGY

Forging a (variant) ElGamal Digital Signature

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

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

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*, $x \mapsto x^x$ mod n, and the *self-power multimap*, x mod $n \mapsto x^x$ mod n.

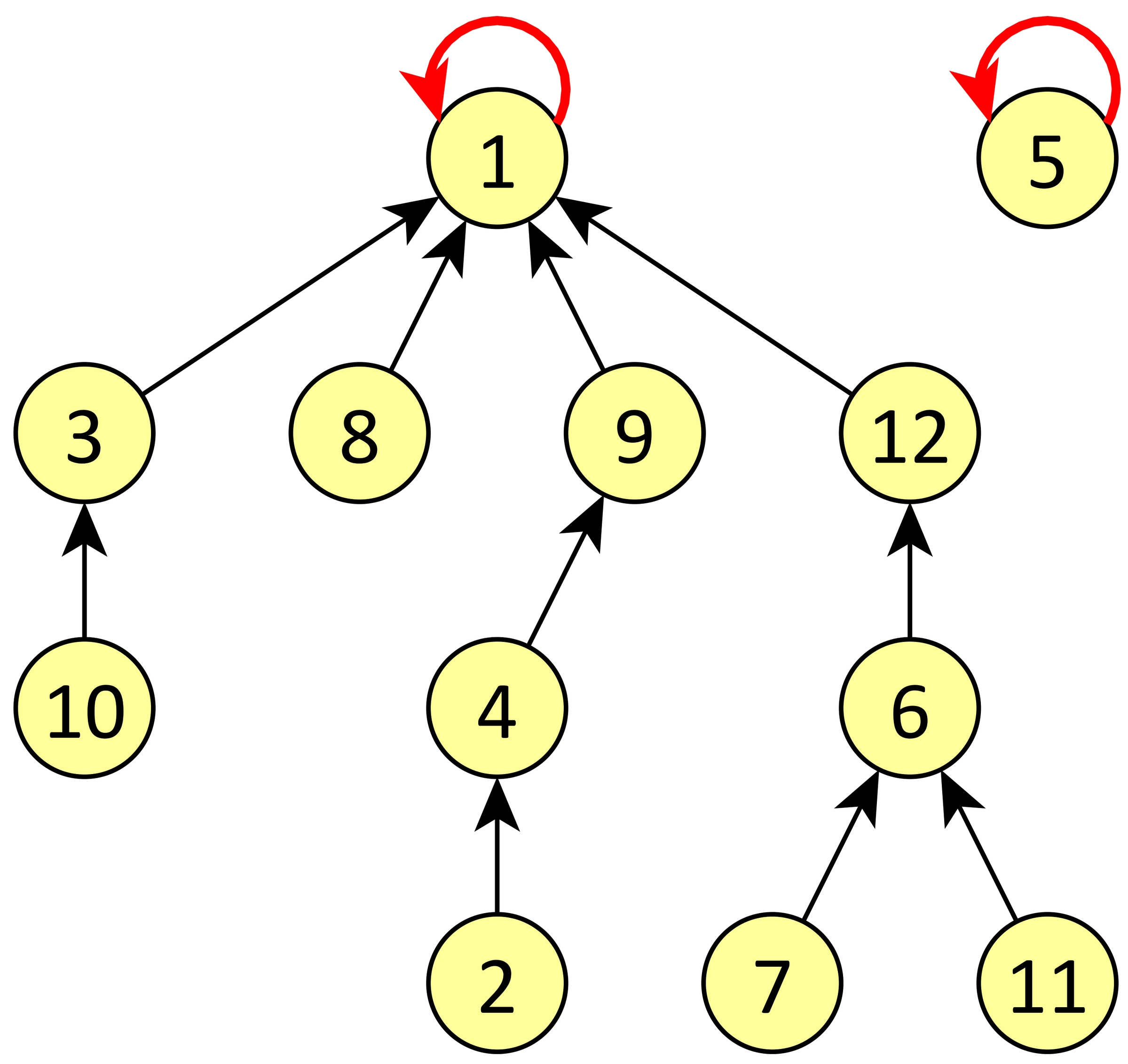

Figure 1: The self-power map modulo 13.

Counting the fixed points and two-cycles

This work investigates:

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

$$x^x \equiv x \pmod{p}, \tag{2}$$

- the number of *two-cycles*, or solutions to

$$h^h \equiv a \pmod{p} \quad \text{and} \quad a^a \equiv h \pmod{p}, \tag{3}$$

- and the corresponding problems modulo prime powers.

1. Solving the prime modulus congruence between 1 and $p-1$

Let $F(p)$ be the number of solutions to (2) such that $1 \le x \le p-1$. We reduce the equation to $x^{x-1} \equiv 1 \pmod{p}$. Then we consider the order of x and of x^{x-1} modulo p. We proceed as in [4] or [1] to prove:

Theorem 1.

$$\left| F(p) - \sum_{n \mid p-1} \frac{\phi(n)}{n} \right| \le d(p-1)^2 \sqrt{p}(1 + \ln p),$$

where $d(p-1)$ is the number of divisors of $p-1$.

2. Solving the prime modulus congruence between 1 and $(p-1)p$

Let $G(p)$ be the number of solutions to (2) with $1 \le x \le (p-1)p$ and $p \nmid x$. Similarly, let $T(p)$ be the number of solutions to (3) with $1 \le h, a \le p(p-1)$, $p \nmid h$, and $p \nmid a$. Using Chinese Remainder Theorem techniques we have:

Theorem 2.

$$G(p) = (p-1) \sum_{n \mid p-1} \frac{\phi(n)}{n}$$

Theorem 3.

$$T(p) = (p-1)^2 \sum_{n \mid p-1} \left(\frac{\phi(n)}{n} \right)^2$$

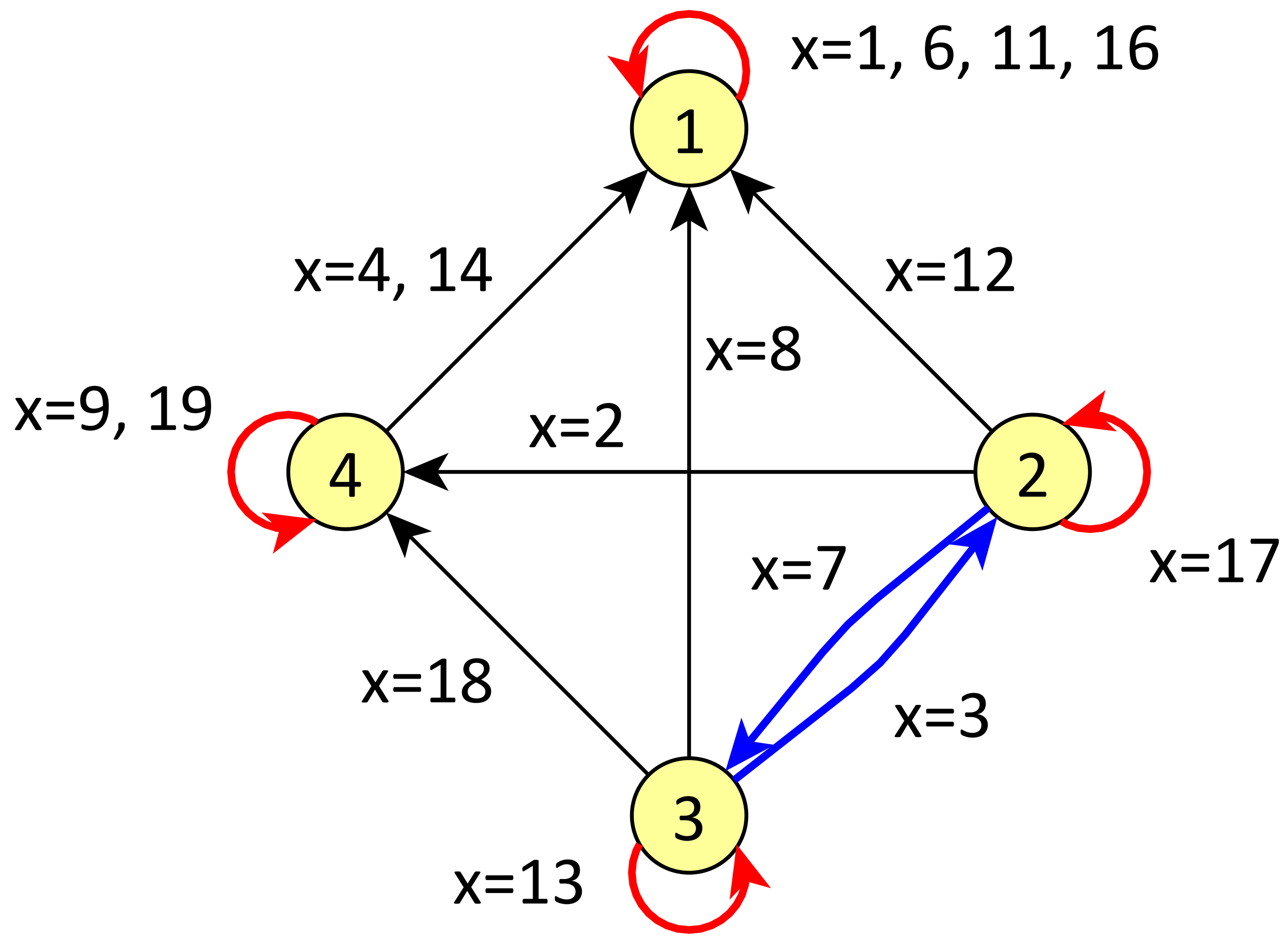

Figure 2: The self-power multimap modulo 5.

3. Solving the prime power congruence between 1 and $(p-1)p^e$

Using the p-adic techniques of [2], we can classify solutions as nonsingular or singular. Each nonsingular solution lifts by Hensel's Lemma to a unique solution modulo p^e. Each singular solution could lift to more than one or none at all.

Theorem 4. *The singular solutions of* (2) *are those with* $x \equiv 1$ *modulo* p. *Each one lifts to* $p^{\lfloor e/2 \rfloor}$ *solutions modulo* p^e. *(This leads to a complete count of solutions modulo* p^e*.)*

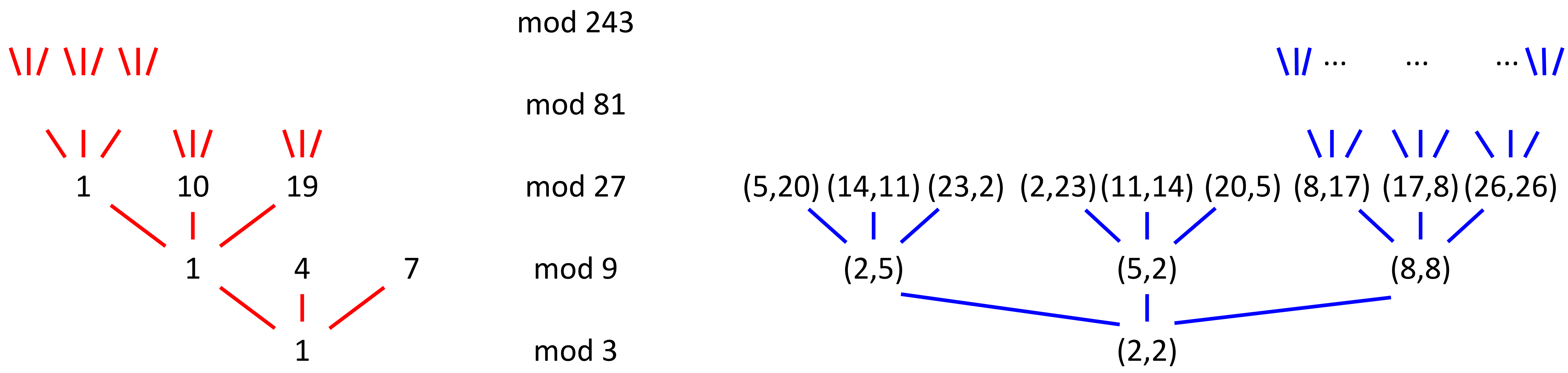

Figure 3: Left: Lifts of a singular fixed point modulo 3^e. Right: Lifts of a singular two-cycle modulo 3^e.

Theorem 5. *The singular solutions of* (3) *are those with* $ha \equiv 1$ *modulo* p. *Each one lifts to* $p^{\lfloor e/2 \rfloor}$ *solutions modulo* p^e *if* $h \not\equiv -1$ *modulo* p *and* $p^{\lfloor e/3 \rfloor + \lfloor (e+1)/3 \rfloor}$ *solutions otherwise.*

The proof uses the Stationary Phase Formula from [3]. Again, this leads to a complete count.

References

[1] Cristian Cobeli and Alexandru Zaharescu, *An Exponential Congruence with Solutions in Primitive Roots*, Rev. Roumaine Math. Pures Appl. **44** (1999), no. 1, 15–22.

[2] Joshua Holden and Margaret M. Robinson, *Counting Fixed Points, Two-Cycles, and Collisions of the Discrete Exponential Function using p-adic Methods*, Journal of the Australian Mathematical Society. Special issue dedicated to Alf van der Poorten, to appear.

[3] J. Igusa, *A Stationary Phase Formula for p-adic Integrals and its Applications*, Algebraic Geometry and its Applications: Collections of Papers from Shreeram S. Abhyankar's 60th Birthday Conference, 1994, pp. 175.

[4] Wen Peng Zhang, *On a Problem of Brizolis*, Pure Appl. Math. **11** (1995), no. suppl., 1–3.