Polynomial Fermat Quotients

Arne Winterhof (RICAM, Austrian Academy of Sciences)

For a prime $p$ and an integer $u$ the Fermat quotient $q_p(u)$ is defined as the unique integer

$$ q_p(u) \equiv \frac{u^{p-1} - 1}{p} \pmod{p}, \quad 0 \leq q_p(u) < p, \text{ if } \gcd(u, p) = 1, $$

and $q_p(u) = 0$ if $\gcd(u, p) = p$. Several number theoretic questions on Fermat quotients and their applications have been studied before, in particular:

1. The smallest $u \geq 1$ with $q_p(u) \neq 0$ is $\leq (\log p)^{463/252 + o(1)}$ (Bourgain et al., 2010).

2. The number of fixed points $0 \leq u < p$ with $q_p(u) = u$ is $O(p^{11/12 + o(1)})$ (Ostafe/Shparlinski, 2011).

3. The image size $\#\{q_p(u) : 0 \leq u < p\}$ is at most $p - \sqrt{(p-1)/2}$ (Vandiver, 1915) and at least $(1 + o(1))p/(\log p)^2$ (Ostafe/Shparlinski, 2011).

4. For any integer $a$, the number of $0 \leq u < p$ with $q_p(u) = a$ is at most $p^{1/2 + o(1)}$ (Fouché, 1986).

5. The number of collisions, that is, $0 \leq u, v, < p$ with $q_p(u) = q_p(v)$, is at most $p^{5/4 + o(1)}$, (Ostafe/Shparlinski, 2011).

Here we study analogous problems for polynomial Fermat quotients defined as follows: Let $q = p^r$ be the power of a prime $p$ and let $\mathbb{F}_q$ denote the finite field of $q$ elements. Fix an irreducible polynomial $P \in \mathbb{F}_q[X]$ of degree $n \geq 2$ and for $A \in \mathbb{F}_q[X]$ we define

$$ q_P(A) \equiv \frac{A^{p^n-1} - 1}{P} \pmod{P}, \quad \deg q_P(A) < n, \text{ if } \gcd(A, P) = 1, $$

and $q_P(A) = 0$ if $\gcd(A, P) = P$. We are especially interested how $q_P$ acts on the set $\mathcal{P}_{n,q}$ of polynomials $A \in \mathbb{F}_q[X]$ of degree at most $n - 1$.

We prove that the number of fixed points of $q_P$ of degree at most $n - 1$ is $O(q^{n/2})$ and we show that the image size $\#\{q_P(A) : A \in \mathcal{P}_{n,q}\}$ of $q_P$ is of order of magnitude $q^{n-1}$. We present some results on the number of polynomials with the same image $\#\{A \in \mathcal{P}_{n,q} : q_P(A) = B\}$ and on the number of collisions $\#\{(A, B) \in \mathcal{P}_{n,q}^2 : q_P(A) = q_P(B)\}$.