Summer 2015 NSERC USRA Research Report: The Congruence Class of X in Quotients of Polynomial Rings of Integers, and Linear Recursive Sequences

Reginald M. Simpson

September 10, 2015

In this project, the multiplicative order of the congruence class of X in rings of the form $\frac{(\mathbb{Z}/m\mathbb{Z})[X]}{(P)}$ was the central object of study. That is to say, the minimal power n such that $X^n \equiv 1 \bmod m, P$.

In order to efficiently discuss the problem, some notation has to be decided upon. Note that *polynomial* shall imply an element whose degree is greater than zero.

Definition 1. The ring $\mathcal{R}_m(P)$ shall denote the following: For a monic polynomial $P \in A[X]$, where $A = \mathbb{Z}$ or $A = \mathbb{Z}_p$:

$$\mathcal{R}_m(P) = \frac{(\mathbb{Z}/m\mathbb{Z})[X]}{(P)} \tag{1}$$

In the case where $A = \mathbb{Z}$, $m \in \mathbb{N}$, $m \geq 2$. In the case where $A = \mathbb{Z}_p$, $m = p^n$, for some $n \in \mathbb{N}$.

Likewise, the element $[x]_{(m,P)}$ will refer in $\mathcal{R}_m(P)$ to the congruence class of X in the polynomial ring containing P. In situations where there is only one polynomial P to choose from, $[x]_m$ will refer to the congruence class of X in $\mathcal{R}_m(P)$.

In order to ensure that the multiplicative order of some $[x]_{(m,P)}$ is well defined, $[x]_{(m,P)}$ must lie in the group of units of $\mathcal{R}_m(P)$. This leads to the neccessary and sufficient condition that $\gcd(m, C) = 1$, where C is the constant coefficient of P. Whenever the order of some $[x]_{(m,P)}$ is discussed, assume (m, P) are chosen such that $[x]_{(m,P)}$ is a unit in the corresponding ring.

The proofs done over the course of this project are sufficient to explain the order of $[x]_{(m,P)}$ for when (1) m is prime, or (2) m is square-free. For powers of primes, some partial results are discussed.

In order to best understand the following statements, keep in mind the fact that an irreducible monic polynomial $P \in sZ_p[X]$, has a reduction $\bar{P} \in \mathbb{F}_p[X]$, $\bar{P} = \bar{S}^e$, where $\bar{S}$ is irreducible in $\mathbb{F}_p[X]$ (see the first two chapters of [Lan94]).

Lemma 1. *For a monic polynomial $P \in \mathbb{Z}[X]$ and integer m, with $m = \prod_{i=1}^{N} p_i^{a_i}$ the prime decomposition of m,* $\operatorname{ord}[x]_{(m,P)} = \operatorname{lcm}(\operatorname{ord}[x]_{(p_1^{a_1},P)}, \ldots, \operatorname{ord}[x]_{(p_N^{a_n},P)})$.

For a monic polynomial $P \in \mathbb{Z}_p[X]$, and power p^n, with $\bar{P} = \prod_{i=1}^{N} \bar{Q}_i^{b_i}$ the decomposition of the reduction of P into irreducible polynomials in $\mathbb{F}_p[X]$, and where for $1 \leq i \leq N$, Q_i is the product of all polynomials dividing P whose reductions have $\bar{Q}_i$ as an irreducible factor, $\operatorname{ord}[x]_{(p^n,P)} = \operatorname{lcm}(\operatorname{ord}[x]_{(p^n,Q_1)}, \ldots, \operatorname{ord}[x]_{(p^n,Q_N)})$,

The consequence of Lemma 1 is that all that is necessary to know the order of any $[x]_{(m,P)}$, is the orders of $[x]$ across the prime factors of m and the irreducible factors of P modulo p.

Now, the following Lemma will partially show how the order of $[x]_{(p,P)}$ influences the order of $[x]$ in rings with higher powers of p.

Lemma 2. *Let $P \in \mathbb{Z}_p[X]$ be a monic polynomial.*

1. *For any $n \in \mathbb{N}$, either* $\operatorname{ord}[x]_{p^{n+1}} = p \operatorname{ord}[x]_{p^n}$, *or* $\operatorname{ord}[x]_{p^{n+1}} = \operatorname{ord}[x]_{p^n}$.
2. *For any $n \in \mathbb{N}$ where $n > 2$ or $p > 2$, if* $\operatorname{ord}[x]_{p^n} = p \operatorname{ord} x_{p^{n-1}}$, *then* $\operatorname{ord}[x]_{p^{n+1}} = p \operatorname{ord}[x]_{p^n}$.
3. *If $p > 2$ and* $\operatorname{ord}[x]_{p^2} = p \operatorname{ord}[x]_p$, *then* $\operatorname{ord}[x]_{p^n} = p^{n-1} \operatorname{ord}[x]_p$.
4. *If* $\operatorname{ord}[x]_8 = 2 \operatorname{ord}[x]_4$, *then for $n \geq 2$,* $\operatorname{ord}[x]_{2^n} = 2^{n-2} \operatorname{ord}[x]_4$.

These statements were proven by noting that in qZp^{n+1} by the binomial expansion, $(1 + kp^n)^p = 1$, for any $k \in \mathbb{Z}/p\mathbb{Z}$.

The relationship between the factorization of P, the discriminant of P, and the order of $[x]_m$ in P is deeply related to the study of the orders of roots of polynomials in finite fields:

Proposition 1. *Let $P = \prod_{i=1}^{N} P_i$ be the partial factorization of some monic $P \in \mathbb{Z}_p[X]$, such that each P_i is pairwise relatively prime modulo p.*

Then it follows that each P_i will be such that there is some irreducible $\bar{S}_i \in \mathbb{F}_p[X]$ such that $\bar{S}_i^{e_i}$ for some $e_i \in \mathbb{N}$.

For each e_i, let k_i denote the minimal integer such that $p^{k_i} \geq e_i$.

Thus:

$$\operatorname{ord}[x]_{(p,P)} = p^{\max\{k_1,\ldots,k_N\}} \operatorname{lcm}(\operatorname{ord}[x]_{(p,S_1)}, \ldots \operatorname{ord}[x]_{(p,S_N)}) \tag{2}$$

For a very short paper that contains statements which are ultimately equivalent to the above proposition, see [FM68].

Moving on to powers of primes, it was found that the cyclotomics had a unique property in terms of order and powers of primes.

Proposition 2. *For a monic polynomial $P \in \mathbb{Z}_p[X]$, P divides $X^\omega - 1$ if and only if for all $n \in \mathbb{N}$ where $p^n > 2$, $\operatorname{ord}[x]_{p^{n+1}} = \operatorname{ord}[x]_{p^n}$.*

This was followed up with the following statement, which has been proven:

Proposition 3. *For a fixed prime p, let $P \in \mathbb{Z}_p[X]$ be an irreducible monic polynomial.*

Let $\omega = \operatorname{ord}[x]_p$.

If p does not divide D, the discriminant of P, there exists a unique $P^\star \in \mathbb{Z}_p[X]$ such that $P \equiv P^\star \bmod P$, $P^\star$ divides X^ω, and $\operatorname{ord}[x]_{p^n} = \operatorname{ord}[x]_p$ if and only if $P \equiv P^\star \bmod p^n$.

One way to think of the above statement is that $\operatorname{ord}[x]_{(p^n,P)}$ depends on the distance between the roots of P and the nearest roots of unity in the algebraic closure of $\mathbb{Q}_p$.

Moving on to linear recursive sequences, it should be mentioned that early in the project, the congruence class of $[x]$ was used to prove statements about the appearance of prime factors in the Fibonacci Sequence.

The relationship between polynomials and linear recursive sequences in the literature is a well-known. The congruence class of $[x]$ in such rings is isomorphic to the action of a function σ known as the shift operator, which acts a linear recursive sequence v_n such that $\sigma v_n = v_{n+1}$ (see [FM68]), with equality between the coefficients of the recursive sequence and the coefficients of the polynomial.

Note that the following $\left(\frac{a}{b}\right)$ is the Legendre symbol. The end result of this, stated without reference to the order of $[x]_p$ is the following:

Proposition 4. *For any prime $p \neq 2, 5$ where $p = 1 \bmod 4$, $F_{(p-\left(\frac{p}{5}\right))/2}$ is the last possible first appearance of p in the Fibonacci Sequence.*

For any prime $p \neq 2, 5$ where $p \equiv 3 \bmod 4$, $F_{(p-\left(\frac{p}{5}\right))}$ is the last possible first appearance of p in the Fibonacci Sequence.

The above can be generalized to all quadratic polynomials (by substituting the discriminant for 5, and considering the special cases where p divides D or $p = 2$ not discussed here, along with some other modifications). This generalization is equivalent to Lucas' statements about prime divisibility in linear recursive sequences.

Some of the most interesting aspects of the problems surrounding the order of the congruence class of X became apparent only in the last month of the research project, and have not had time to bear any complete results. In particular the question of the multiplicative order of the congruence class of X is deeply tied into the structure of the decomposition of the cyclotomic polynomials in the p-adic integers, and the distribution of the roots of unity in the p-adic numbers.

References

[FM68] Jay P. Fillmore and Morris L. Marx, *Linear recursive sequences*, SIAM Review **Vol. 10, No. 3** (1968), 342–353.

[Lan94] Serge Lang, *Algebraic number theory*, Springer-Verlag, 175 5th Avenue, New York, 1994.