CHAINS OF CONGRUENCES IN RINGS OF INTEGERS

AUTHOR

Abstract

We explore the chain $x^{n^m} \equiv \cdots \equiv x^a \equiv x^{a-1} \pmod{n}$ where n, m, a are positive integers. First, we find a such a chain when n is a prime or prime power. Then, we determine when a chain exists for a composite n. We do this for composites which are a product of two distinct primes, k distinct primes, and two distinct prime powers to build up to the solution for a general n. We establish this chain through a focus on the expression $x^{n^a} - x^{n^{a-1}} \pmod{n}$ and prime factors of n. After proving when such a chain exists in $\mathbb{Z}/n\mathbb{Z}$, we generalize to rings of integers of number fields using a similar process.

Introduction

It's a well known and common idea in elementary number theory courses that $x^p - x$ vanishes on all elements of $\mathbb{Z}_p = \mathbb{Z}/p\mathbb{Z}$. That is, $x^p - x \equiv 0 \pmod{p} \forall x \in \mathbb{Z}_p$ due to Fermat's Little Theorem. When we look at finite fields $\mathbb{F}_q$, we see that $x^q - x = 0$ for all $x \in \mathbb{F}_q$, so the notion of vanishing still exists here. What if we could find a somewhat similar expression for $\mathbb{Z}_{p^n}$? $x^{p^n} - x^{p^{n-1}} \pmod{p^n}$ is a simple generalization from $\mathbb{Z}_p$ to $\mathbb{Z}_{p^n}$, so when does $x^{p^n} - x^{p^{n-1}} \equiv 0 \pmod{p^n}\ \forall x \in \mathbb{Z}/p^n\mathbb{Z}$ for some prime p and integer $n > 0$? Or even more general: does $x^{p^a} - x^{p^{a-1}} \equiv 0 \pmod{p^n}\ \forall x \in \mathbb{Z}/p^n\mathbb{Z}$ for $a \geq n$? What if we could generalize to composite n? That is, when does $x^{n^a} - x^{n^{a-1}} \equiv 0 \pmod{n}$ for some $a > 1$? All of these examples involve only $\mathbb{Z}/n\mathbb{Z}$, so what if we looked at a number field K and took its ring of integers $\mathcal{O}_K$? In particular, when does a chain exist for $\mathcal{O}_K/n\mathcal{O}_K$? In this paper, we answer these questions using an elementary approach. To look at these questions in a different way, we're examining roots of the binomial $x^{n^a} - x^{n^{a-1}} \pmod{n}$ for some $a, b \in \mathbb{Z}$. This would mean that the binomial *vanishes* on $\mathbb{Z}/n\mathbb{Z}$.

In [5], the authors determined a basis for the set of polynomials vanishing on $\mathbb{Z}/n\mathbb{Z}$. We will determine when the binomial vanishes, but not resort to expressing the binomial in terms of generators. In [6], the author corrected a statement in [5] and generalized the results to commutative rings. Similarly, we will generalize the vanishing of the binomial to rings of integers of number fields. In particular, from varying a, we will verify when the following paper-specific definitions hold for factor rings of integer rings.

Definition 1. When every $x \in \mathbb{Z}/n\mathbb{Z}$ is a root of $x^{n^a} - x^{n^{a-1}} \pmod{n}$, we will say there is a *chain* modulo n or $\mathbb{Z}/n\mathbb{Z}$ *exhibits a chain*. In particular, we have a chain

$$x^{n^a} \equiv x^{n^{a-1}} \equiv \cdots \equiv x^{n^m} \pmod{n}$$

where m is the smallest integer such that the binomial $x^{n^a} - x^{n^m} \equiv 0 \pmod{n}\ \forall x \in \mathbb{Z}/n\mathbb{Z}$.

Remark 2. When we generalize to rings of integers $\mathcal{O}_K$ for some number field K, we let $X \in \mathcal{O}_K/\mathfrak{n}$ where $\mathfrak{n} \trianglelefteq \mathcal{O}_K$ meaning $\mathfrak{n}$ is an ideal of $\mathcal{O}_K$. We also define $N(\mathfrak{n})$ to be the ideal norm. Now when every $X \in \mathcal{O}_K/\mathfrak{n}$ satisfies $X^{N(\mathfrak{n})^a} - X^{N(\mathfrak{n})^{a-1}} \equiv 0 \pmod{\mathfrak{n}}$ we say that $\mathcal{O}_K/\mathfrak{n}$ exhibits a chain

$$X^{N(\mathfrak{n})^a} \equiv X^{N(\mathfrak{n})^{a-1}} \equiv \cdots \equiv X^{N(\mathfrak{n})^m} \pmod{\mathfrak{n}}$$

where again m is the smallest integer such that $X^{N(\mathfrak{n})^a} - X^{N(\mathfrak{n})^m} \equiv 0 \pmod{\mathfrak{n}}\ \forall X \in \mathcal{O}_K/\mathfrak{n}$

Throughout the article, we break up the results into a few sections. in the first section of results, we find that $\mathbb{Z}/p\mathbb{Z}$ and $\mathbb{Z}/p^n\mathbb{Z}$ both exhibit chains for some prime p and $n \in \mathbb{Z}^+$. In the second section, we go into some cases of composite n, namely, $n = pq$ for distinct primes p, q and $n = p_1 \cdots p_k$ for distinct primes $p_1, \ldots, p_k$. In the third section, we examine the case of $n = p^\alpha q^\beta$ for distinct primes p, q and $\alpha, \beta \in \mathbb{Z}^+$. The results of that case provide a glimpse into one of the main theorems of the paper. We will show the following:

Theorem 9. *Let $n = p_1^{\alpha_1} \cdots p_k^{\alpha_k}$ be a product of k distinct prime powers where all the $\alpha_i \in \mathbb{Z}^+$ for $1 \leq i \leq k$. Then $x^{n^a} - x^{n^{a-1}} \equiv 0 \pmod{n}\ \forall x \in \mathbb{Z}/n\mathbb{Z} \iff (p_i - 1) \mid (n/p_i^{\alpha_i})^a - (n/p_i^{\alpha_i})^{a-1}$*

In the final section of results, we generalize **Theorem 9** to factor rings of integer rings. This generalization gives us the final theorem for the paper.

Theorem 11. *Let $\mathcal{O}_K$ be the ring of integers for a number field K and $I = \mathfrak{n} \trianglelefteq \mathcal{O}_K$ with $\mathfrak{n} = \mathfrak{p}_1^{\alpha_1} \cdots \mathfrak{p}_k^{\alpha_k}$ for nonzero prime ideal $\mathfrak{p}_i$ and $\alpha_i \in \mathbb{Z}$. Then we have a chain*

$$X^{N(\mathfrak{n})^m} \equiv \ldots \equiv X^{N(\mathfrak{n})^{a-1}} \pmod{\mathfrak{n}}\ \forall X \in \mathcal{O}_K/I$$

$$\iff$$

$$(N(\mathfrak{p}_i) - 1) \mid (N(\mathfrak{n})/N(\mathfrak{p}_i))^a - N(\mathfrak{n})/N(\mathfrak{p}_i))^{a-1})$$

for $m, a \in \mathbb{Z}^+$

Background Definitions and Theorems

In the results, we assume the knowledge of the below ideas and other related concepts. For less experienced readers, the preliminary definition and theorems will be crucial in understanding the results. For further knowledge and proofs of the below ideas, we refer the reader to [1] and [2].

Fermat's Little Theorem: Let $a \in \mathbb{Z}_p$ such that $\gcd(a, p) = 1$. Then $a^{p-1} \equiv 1 \pmod{p}$. This also implies that $a^p \equiv a \pmod{p}$. Note that it necessarily follows that $\text{ord}_p(a) \mid (p - 1)$

Definition 2: The *Euler Totient Function* of n, denoted $\varphi(n)$, is the number of positive integers a less than n such that

$\gcd(a, n) = 1$. That is, $\varphi(n) = |\{a \in \mathbb{Z}_n | \gcd(a, n) = 1\}|$.

Euler's Theorem: Let $a \in \mathbb{Z}_n$ such that $\gcd(a, n) = 1$. Then $a^{\varphi(n)} \equiv 1 \pmod{n}$. Just like which Fermat's Little Theorem, we see that $\text{ord}_n(a) \mid \varphi(n)$.

Chinese Remainder Theorem: Let $n_1, \ldots, n_k \in \mathbb{Z}$ with $P = n_1 \cdots n_k$. If $\gcd(n_i, n_j) = 1$ for every $i \neq j$ and if $a_1, \ldots, a_k \in \mathbb{Z}$ with $a_i \in \mathbb{Z}_{n_i}$, then there exists a unique solution $x \in \mathbb{Z}/P\mathbb{Z}$ satisfying

$$\begin{aligned} x &\equiv a_1 \pmod{n_1} \\ x &\equiv a_2 \pmod{n_2} \\ &\vdots \\ x &\equiv a_k \pmod{n_k} \end{aligned}$$

In a more abstract sense, we have an isomorphism $\mathbb{Z}/P\mathbb{Z} \cong \bigoplus_{i=1}^{k} \mathbb{Z}/n_i\mathbb{Z}$.

The above are the elementary ideas required to follow the bulk of the paper. The next few definitions are meant to understand generalizations to rings of integers of a number field, so more background knowledge is assumed. For avid readers, we refer them to [3], specifically Chapter 1, or [4] Chapters 1 and 2.

Definition 3: An *Integral Domain* R is a nonzero commutative ring in which the product $ab = 0 \iff a = 0$ or $b = 0$ for all $a, b \in R$. A common example of this is $\mathbb{Z}$.

Definition 4: A *Dedekind Domain* is an Integral Domain with the property that every Ideal I factors into a unique product of prime ideals. An example of a Dedekind domain is the ring of integers $\mathcal{O}_K$ for some number field K.

Generalized Euler's Theorem for Rings of Integers: Let $\mathcal{O}_K$ be the ring of integers for a number field K and let $\mathfrak{n}$ be an ideal of $\mathcal{O}_K$. If $a \in \mathcal{O}_K/\mathfrak{n}$ with $a \in (\mathcal{O}_K/\mathfrak{n})^\times$, then $a^{\varphi(\mathfrak{n})} \equiv 1 \pmod{\mathfrak{n}}$. Here we define the totient function to be

$$\varphi(\mathfrak{n}) = \prod_{i=1}^{k} \varphi(\mathfrak{p}_i^{\alpha_i})$$

and $\varphi(\mathfrak{p}_i^{\alpha_i}) = N(\mathfrak{p})^{\alpha_i - 1}(N(\mathfrak{p}) - 1)$ where N is ideal norm.

Chinese Remainder Theorem for Dedekind Domains: Let D be a Dedekind Domain with ideals $I_1, \ldots, I_n$ with $I = \prod_{j=1}^{n} I_j$. If I_j, I_k are coprime for $j \neq k$ with $1 \leq j, k \leq n$, then we have an isomorphism

$$D/I \cong \bigoplus_{j=1}^{n} D/I_j$$

Results

1. n is a prime or prime power

Proposition 1. *$\forall x \in \mathbb{Z}/p\mathbb{Z},\ x^{p^a} - x^{p^{a-1}} \equiv 0 \pmod{p}$ where $p \in \mathbb{Z}$ is prime. In particular, there exists a chain $x^{p^a} \equiv x^{p^{a-1}} \equiv \cdots \equiv x \pmod{p}$.*

Proof. Note that $x^{p^a} \equiv (x^{p^{a-1}})^p \equiv x^{p^{a-1}} \pmod{p}$ by Fermat's Little Theorem. Since a was arbitrary, we know that such a chain exists and we are done. □

While for primes p, we have that the chain continues to x, this is only due to Fermat's Little Theorem. Therefore, when dealing with composite n, we won't have a chain extending from x^{n^a} down to x unless n is a Carmichael number. One take away from **Proposition 1** is that we only need to examine when $x^{n^a} \equiv x^{n^{a-1}} \pmod{n}$ to find our chain since keeping a arbitrary constructs the chain implicitly. Now that we've established the chain for primes, we move on to prime powers, but this requires an establishment of a more unique property of $\mathbb{Z}_{p^\alpha}$ for some $\alpha \in \mathbb{Z}^+$ and a somewhat trivial graphical idea.

Lemma 2. *For all positive integers α, p, $p^{\alpha-1} \geq \alpha$.*

Proof. This can be easily seen through a graphical comparison of $f(x) = x$ and $g(x) = p^{x-1}$ for some prime p. For odd primes, the only intersection point is $x = 1$, but then g is strictly greater than f. For $p = 2$, we get two intersection points of $x = 1$ and $x = 2$. When looking at integer lattice points, for $x \geq 2$, g is once again strictly greater than f. □

Proposition 3. *There exists a chain $x^{p^m} \equiv \cdots \equiv x^{p^n} \equiv x^{p^{n-1}} \pmod{p^n}$ $\forall x \in \mathbb{Z}/p^n\mathbb{Z}$ where $m, n \in \mathbb{Z}^+$ such that $m \geq n$.*

Proof. Due to the well ordering of the Integers, we can write $m = n + k$ for some integer $k \geq 0$. Now we just need to show that $x^{p^{n+k}} - x^{p^{n+k-1}} \equiv 0 \pmod{p^n}$ for all $x \in \mathbb{Z}_{p^n}$. We can factor to get:

$$x^{p^{n+k}} - x^{p^{n+k-1}} = x^{p^{n+k-1}}(x^{p^{n+k-1}(p-1)} - 1) \tag{1}$$

$$= x^{p^{n+k-1}}(x^{\varphi(p^n)p^k} - 1) \tag{2}$$

Euler's Theorem gives that all non-multiples of p are roots of the expression, and $p^n \mid (kp)^{p^{n+k-1}}$ since $p^{n+k-1} \geq n$. Then we conclude that $x^{p^{n+k}} - x^{p^{n+k-1}} \equiv 0 \pmod{p^n}$ for all $x \in \mathbb{Z}_{p^n}$. Now we can expand this result to get a chain of congruences like we did in **Proposition 1**. In particular, changing the k values gets us the desired chain and we have a chain from x^{p^m} down to $x^{p^{n-1}}$ □

While the expression seems very similar, it is very different in that we aren't raising our modulo to a power, but rather, we are looking at $x^{p^{n-1}}$. One can see that that $x^{p^{n-1}} \equiv x^{p^{n-2}} \pmod{p^n}$ is not necessarily true for all primes p. For example, mod 8, $6^4 \not\equiv 6^2 \pmod{8}$. We now expand this result to the chain for prime powers.

Using this result, we can state that $x^{n^m} \equiv \cdots \equiv x^n \pmod{n}$ where n is a prime power and $m \in \mathbb{Z}$ which gives us the necessary conclusions for this section.

2. n as a product of distinct primes

We begin this section with a useful lemma which is commonly covered in a standard number theory or abstract algebra course or book. This idea will be particularly useful in this section.

Lemma 4. *Let $a, k \in \mathbb{Z}$ such that $k \geq \varphi(n)$, $\gcd(a, n) = 1$, and $a^k \equiv 1 \pmod{n}$ for all nonzero integers a. Then $a^k \equiv 1 \pmod{n} \iff \varphi(n) \mid k$*

Proof. ($\Rightarrow$) Let $l = \text{ord}_n(a)$ be the order of $a \in \mathbb{Z}_n$ and let $k \in \mathbb{Z}$ such that $a^k \equiv 1 \pmod{n}$ for all nonzero $a \in \mathbb{Z}_n$. Suppose for contradiction, that $\varphi(n) \nmid k$. Then $k = \varphi(n)q + r$ for $0 < r < \varphi(n)$. At the same time note that $\varphi(n) \nmid k \implies l \nmid k$ since $l \mid \varphi(n)$ meaning $k = l(tq) + r$ and $0 < r < l$ for some $t \in \mathbb{Z}$. Then $a^k \equiv a^{\varphi(n)q+r} \equiv a^r \equiv 1 \pmod{n}$. However, due to the definition of order, we have that $r = 0$ since $r < l$. This means that $k = l(tq) = \varphi(n)q \implies \varphi(n) \mid k$.
($\Leftarrow$) Suppose $\varphi(n) \mid k$. Then $k = \varphi(n)q$ for some $q \in \mathbb{Z}^+$, and $a^k \equiv a^{\varphi(n)q} \equiv 1^q \equiv 1 \pmod{n}$. □

Now we can go ahead and move into the main ideas for this section. One can quickly see that there is a focus on prime numbers throughout the paper along with a reliance on the previous lemma and Chinese Remainder Theorem. Let's look at some composite n examples through a table first. The n below are the product of two distinct primes. We see that $6, 10, 21$ are examples of such n, but why? The next proposition reveals the answer.

Table 1. Chains for Composite $n = pq$

n	Chain?
6	Yes, for $a > 1$
10	Yes, for $a > 2$
14	Doesn't appear to be
15	Also doesn't appear to be
21	Yes, for $a > 1$

Proposition 5. *Let $n = pq$ where $p, q \in \mathbb{Z}$ are distinct primes. Then $x^{n^a} - x^{n^{a-1}} \equiv 0 \pmod{n} \forall x \in \mathbb{Z}/pq\mathbb{Z} \iff (p-1) \mid \varphi(q^a)$ and $(q-1) \mid \varphi(p^a)$.*

Proof. Substituting $n = pq$ into our expression, we have: $x^{(pq)^a} - x^{(pq)^{a-1}} = (x^{p^a})^{q^a} - (x^{p^{a-1}})^{q^{a-1}}$. Note that exponents are commutative so the expression is equivalent to $(x^{q^a})^{p^a} - (x^{q^{a-1}})^{p^{a-1}}$. Using Chinese Remainder Theorem,

$$(x^{p^a})^{q^a} \equiv (x^{p^{a-1}})^{q^{a-1}} \pmod{pq}$$
$$\iff (x^{p^a})^{q^a} \equiv (x^{p^{a-1}})^{q^{a-1}} \pmod{p}$$
$$\text{and } (x^{q^a})^{p^a} \equiv (x^{q^{a-1}})^{p^{a-1}} \pmod{q}$$

Now suppose that this congruence is indeed true. Then **Corollary 2** implies that we should have

$$x^{q^a} \equiv x^{q^{a-1}} \pmod{p} \text{ and } x^{p^a} \equiv x^{p^{a-1}} \pmod{q}$$

Since every element, except 0, has an inverse modulo a prime, we can reduce this expression to

$$x^{(q-1)q^{a-1}} \equiv 1 \pmod{p} \text{ and } x^{(p-1)p^{a-1}} \equiv 1 \pmod{q}$$

if and only if $(p-1) \mid [(q-1)q^{a-1}] = \varphi(q^a)$ and $(q-1) \mid [(p-1)p^{a-1}] = \varphi(p^a)$ by **Lemma 4**. □

The next idea reveals yet another way to find $n = pq$ for which we find a chain.

Corollary 6. *Let $p, q \in \mathbb{Z}$ be prime numbers. $(p-1) \mid \varphi(q^a)$ and $(q-1) \mid \varphi(p^a) \iff q = p^\alpha - p^{\alpha-1} + 1$ for some integer $\alpha \leq a$.*

Proof. WLOG, let $p < q$ and suppose we have two primes p, q such that $(p-1) \mid \varphi(q^a)$ and $(q-1) \mid \varphi(p^a)$. Then $(p-1) \mid \varphi(q^a) \iff (p-1) \mid (q-1)$ since $\gcd(p-1, q) = 1$. Now we can say $q - 1 = k(p-1)$ for some $k \in \mathbb{Z}$. Continuing, $(q-1) \mid \varphi(p^a) \iff k \mid p^{a-1} \iff k = p^t$ where $t \leq a-1$. Knowing these ideas, we see $q = p^t(p-1) + 1 = p^{t+1} - p^t + 1$ and the specific $\alpha = t + 1$ and we are done. □

Now, instead of having properties defined by divisibility, we can look at this case using a polynomial. Combining **Corollary 6** with **Proposition 5**, we have the following table. While many of the values don't have chains for $a = 2$,

Table 2. Chains for Composite $n = pq$ and $a = 2$

n	Chain?
6	Yes
10	No
14	No
15	No
21	Yes
22	No
26	No

upon inspection, one can see that increasing the a value adds new n to our list. For example, when $a = 3$, we add $n = 10$ and $n = 57$ to our list. Now that we've examined the $n = pq$ case, we can look at n as a product of k distinct primes.

Proposition 7. *Let $n = p_1 \cdots p_k$ where the $p_i \in \mathbb{Z}$ are distinct primes for $1 \leq i \leq k$. Then $x^{n^a} - x^{n^{a-1}} \equiv 0 \pmod{n}$ $\forall x \in \mathbb{Z}/n\mathbb{Z} \iff \varphi(p_i^a) \mid n^{a-1}(n/p_i - 1)$.*

Proof. Like before, we can use Chinese Remainder Theorem to look at the expression modulo each p_i. Using Proposition 1, we get that $x^{n^a} - x^{n^{a-1}} \equiv x^{(n/p_i)^a} - x^{(n/p_i)^{a-1}} \equiv \pmod{p_i}$. Suppose $x^{n^a} - x^{n^{a-1}} \equiv 0 \pmod{n}$, then continuing from the previous line:

$$x^{(n/p_i)^a} \equiv x^{(n/p_i)^{a-1}} \pmod{p_i}$$

Since every nonzero element of $\mathbb{Z}_{p_i}$ has an inverse, we can write

$$x^{(n/p_i)^a-(n/p_i)^{a-1}} \equiv 1 \pmod{p_i}$$

$$\iff (p_i-1) \mid ((n/p_i)^a-(n/p_i)^{a-1})$$

by **Lemma 4**. We can factor $(n/p_i)^a-(n/p_i)^{a-1}=(n/p_i)^{a-1}(n/p_i-1)$. In particular, we must have

$$\frac{n^{a-1}(\frac{n}{p_i}-1)}{p_i^{a-1}(p_i-1)}=\frac{n^{a-1}(\frac{n}{p_i}-1)}{\varphi(p_i^a)} \in \mathbb{Z}$$

and we are done. □

Let us look at two examples above the above proposition.

Example 1: $n=30$ with $a=3$

Clearly $(2-1) \mid (15)^2(14)$ and $(3-1) \mid (10)^2(9)$. Checking the last prime, we see $4 \mid (6)^2(5)$ and $6^2=36=4\cdot 9$ so $n=30$ exhibits a chain for $a \geq 3$.

We can confidently say that $n=30$ works for $a>3$ since for larger a we can isolate the $a=3$ case. So for instance, if $a=4$, we verify if $(p_i-1) \mid (n/p_i)^3(n/p_i-1)=(n/p_i)(n/p_i)^2(n/p_i-1)$. Note that since n was arbitrary we can generalize this to all n that exhibit a chain for some a. That is, if n exhibits a chain for some a, it exhibits a chain for all $b>a$.

3. n as a product of prime powers

The next few proofs delve into more casework since in the case of prime moduli p, every positive $a \in \mathbb{Z}_p$ has $\gcd(a,p)=1$ so we can neatly assume the existence of inverses in $\mathbb{Z}_p$. In the case of $\mathbb{Z}_{p^\alpha}$, we have two cases of when $\gcd(a,p)=1$, where we can use Euler's theorem, and when $\gcd(a,p)\neq 1$, where the solution is quite simple since $a=kp$ for some $k \in \mathbb{Z}$.

First, we will examine the case of n as a product of two distinct prime powers to gain an idea of how to answer the general case. Then we look at the case where n is any number to finish off the results.

Like before, we will look at a table of values with $n=p^\alpha q^\beta$ for primes p,q where $\alpha,\beta>0$ but it may be the case where only either $\alpha>1$ or $\beta>1$. In Table 3, we see that there are plenty of n satisfying our conditions while n not exhibiting a chain appear to be rare. Now we see what exactly allows such n to be a chain.

Proposition 8. *Let $n=p^\alpha q^\beta$ where $p,q \in \mathbb{Z}$ are prime and $\alpha,\beta \in \mathbb{Z}^+$. Then $x^{n^a}-x^{n^{a-1}} \equiv 0 \pmod{n}$ $\forall x \in \mathbb{Z}/n\mathbb{Z}$ $\iff$ $(p-1) \mid q^{\beta a}-q^{\beta(a-1)}$ and $(q-1) \mid p^{\alpha a}-p^{\alpha(a-1)}$*

Proof. Let $P=p^\alpha$ and $Q=q^\beta$ to reduce notational complexity. Using Chinese Remainder Theorem we see

$$x^{(PQ)^a}-x^{(PQ)^{a-1}} \equiv x^{Q^a p^{\alpha-1}}-x^{Q^{a-1}p^{\alpha-1}} \pmod{p^\alpha} \tag{1}$$

Table 3. Chains for Composite $n = p^\alpha q^\beta$ and $a = 3$

n	Chain?
12	Yes
18	Yes
20	Yes
24	Yes
21	Yes

using **Proposition 3**. Now suppose this congruence is true. We have two cases: one where $\gcd(x, n) = 1$ and one where $\gcd(x, n) \neq 1$. Let's progress assuming the first case so suppose we have $x \ni \gcd(x, n) = 1$. Then we can progress using inverses like so.

$$x^{Q^a p^{\alpha-1}} - x^{Q^{a-1} p^{\alpha-1}} \equiv 0 \pmod{p^\alpha} \tag{2}$$

$$\iff x^{Q^a p^{\alpha-1}} = x^{Q^{a-1} p^{\alpha-1}} \pmod{p^\alpha} \tag{3}$$

$$\iff x^{Q^a p^{\alpha-1} - Q^{a-1} p^{\alpha-1}} \equiv 1 \pmod{p^\alpha} \tag{4}$$

$$\iff \varphi(p^\alpha) \mid Q^a p^{\alpha-1} - Q^{a-1} p^{\alpha-1} \tag{5}$$

Note that the final result in (5) can be simplified. We see

$$\frac{Q^a p^{\alpha-1} - Q^{a-1} p^{\alpha-1}}{\varphi(p^\alpha)} = \frac{Q^a p^{\alpha-1} - Q^{a-1} p^{\alpha-1}}{p^{\alpha-1}(p-1)} = \frac{q^{\beta a} - q^{\beta(a-1)}}{p-1} \tag{6}$$

so we've reduced the question of whether $\varphi(p^\alpha) \mid Q^a p^{\alpha-1} - Q^{a-1} p^{\alpha-1}$ to whether $(p-1) \mid q^{\beta a} - q^{\beta(a-1)}$. Using the same steps, we can achieve the same conclusion when reducing modulo q^β. That is, analogously, we must also have $(q-1) \mid p^{\alpha a} - p^{\alpha(a-1)}$. Now let's consider when $\gcd(x, n) \neq 1$. If $\gcd(x, n) \neq 1$, x is either a multiple of p or a multiple of q or both. Let $x = kp$ for $k \in \mathbb{Z}$. Clearly

$$(kp)^{Q^a p^{\alpha-1}} \equiv (kp)^{Q^{a-1} p^{\alpha-1}} \equiv 0 \pmod{p^\alpha} \tag{7}$$

by **Lemma 2**. Considering the expression modulo q^β, if $k = q$, we are done since the expression would be congruent to 0. When $k \neq q$, we have $\gcd(x, q) = 1$ meaning we arrive at the conclusion of

$$(kp)^{P^a q^{\beta-1}} \equiv (kp)^{P^{a-1} q^{\beta-1}} \equiv 0 \pmod{q^\beta} \tag{8}$$

$$\iff (q-1) \mid p^{\alpha a} - p^{\alpha(a-1)} \tag{9}$$

like we did before. We can use the same logic for the other case of reducing modulo p^α. As a result, we see that whether $\gcd(x, n) = 1$ or not, we must have

$$(p-1) \mid q^{\beta a} - q^{\beta(a-1)} \text{ and } (q-1) \mid p^{\alpha a} - p^{\alpha(a-1)}$$

to guarantee $x^{n^a} - x^{n^{a-1}} \equiv 0 \pmod{n}$ $\forall x \in \mathbb{Z}_n$ where $n = p^\alpha q^\beta$ as defined earlier. □

Now that we've finished this initial proof, we can generalize to any composite n, but first, we will look at some examples using the results of **Proposition 8**.

Example 3: $n = 45$ with $a = 3$.

From the prime factorization of 45, we see that $45 = (3^2)(5)$. Using this, checking the $p = 3$ case, we have $5^3 - 5^2 = 100$ which is even so $(3-1) \mid 100$. For $p = 5$, we have $3^6 - 3^4 = 3^4(9-1) = 3^4(8)$ meaning $(5-1) \mid 3^4(8)$ so $n = 45$ works for $a \geq 3$.

Next, we prove the one of the main results of the paper, which is a culmination of the previous ideas described. After the proof, we will also display the main algorithm to compute $n \in \mathbb{Z}$ for which there exists a chain $x^{n^m} \equiv \cdots \equiv x^{n^{a-1}} \pmod{n}$ for some $a \in \mathbb{Z}^+$.

Theorem 9. *Let $n = p_1^{\alpha_1} \cdots p_k^{\alpha_k}$ be a product of k distinct prime powers where all the $\alpha_i \in \mathbb{Z}^+$ for $1 \leq i \leq k$. Then $x^{n^a} - x^{n^{a-1}} \equiv 0 \pmod{n}\ \forall x \in \mathbb{Z}/n\mathbb{Z} \iff (p_i - 1) \mid (n/p_i^{\alpha_i})^a - (n/p_i^{\alpha_i})^{a-1}$*

Proof. Using Chinese Remainder Theorem, we can reduce our expression like so,

$$x^{n^a} - x^{n^{a-1}} \equiv (x^{(n/p_i^{\alpha_i})^a})^{p_i^{\alpha_i - 1}} \tag{1}$$

$$- (x^{(n/p_i^{\alpha_i})^{a-1}})^{p_i^{\alpha_i - 1}} \pmod{p_i^{\alpha_i}} \tag{2}$$

using **Proposition 4**. Like in the previous proposition, we move forward with two cases: one with $\gcd(x, p_i) = 1$ and one with $\gcd(x, p_i) \neq 1$ so $x = kp_i$ for some $k \in \mathbb{Z}$. Suppose that the expression is congruent to 0 and $\gcd(x, p_i) = 1$. Then we have

$$(x^{(n/p_i^{\alpha_i})^a})^{p_i^{\alpha_i - 1}} = (x^{(n/p_i^{\alpha_i})^{a-1}})^{p_i^{\alpha_i - 1}} \pmod{p_i^{\alpha_i}} \tag{3}$$

Now we flip the multiplication of the exponents and then use the existence of inverses to continue giving us

$$(x^{p_i^{\alpha_i - 1}})^{(n/p_i^{\alpha_i})^a} \equiv (x^{p_i^{\alpha_i - 1}})^{(n/p_i^{\alpha_i})^{a-1}} \pmod{p_i^{\alpha_i}} \tag{4}$$

$$\iff (x^{p_i^{\alpha_i - 1}})^{(n/p_i^{\alpha_i})^a - (n/p_i^{\alpha_i})^{a-1}} \equiv 1 \pmod{p_i^{\alpha_i}} \tag{5}$$

The result of (3) allows us to use **Lemma 4** and see

$$(x^{p_i^{\alpha_i - 1}})^{(n/p_i^{\alpha_i})^a - (n/p_i^{\alpha_i})^{a-1}} \equiv 1 \pmod{p_i^{\alpha_i}} \tag{6}$$

$$\iff \varphi(p_i^{\alpha_i}) \mid \left(p_i^{\alpha_i - 1}\left((n/p_i^{\alpha_i})^a - (n/p_i^{\alpha_i})^{a-1}\right)\right) \tag{7}$$

Simplifying (4), we get the result

$$\frac{p_i^{\alpha_i - 1}\left((n/p_i^{\alpha_i})^a - (n/p_i^{\alpha_i})^{a-1}\right)}{p_i^{\alpha_i - 1}(p-1)} = \frac{(n/p_i^{\alpha_i})^a - (n/p_i^{\alpha_i})^{a-1}}{p_i - 1} \tag{8}$$

so following from (5), we see

$$x^{n^a} - x^{n^{a-1}} \equiv 0 \pmod{n} \iff (p_i - 1) \mid (n/p_i^{\alpha_i})^a - (n/p_i^{\alpha_i})^{a-1} \tag{9}$$

as desired. Now we must prove that the polynomial vanishes when $x = kp_i$ as defined earlier. Much like previous propositions, this case is trivial due to the magnitude of the exponents we are working in. That is,

$$((kp_i)^{p_i^{\alpha_i-1}})^{(n/p_i^{\alpha_i})^a} \equiv ((kp_i)^{p_i^{\alpha_i-1}})^{(n/p_i^{\alpha_i})^{a-1}} \equiv 0 \pmod{p_i^{\alpha_i}} \tag{10}$$

by **Lemma 2** so $x^{n^a} - x^{n^{a-1}} \equiv 0 \pmod{n}$ regardless of the $\gcd(x, n)$ and we only need to verify when $(p_i - 1) \mid (n/p_i^{\alpha_i})^a - (n/p_i^{\alpha_i})^{a-1}$ for general composite n. □

Remark: If we simply reduced mod p_i, we would get the same result, but this disobeys Chinese Remainder Theorem which is interesting.

Generalization to Rings of Integers

Here we attempt to generalize results from $\mathbb{Z}/n\mathbb{Z}$ to rings of integers over an ideal. In particular, let K be a number field and let $\mathcal{O}_K$ be the ring of integers of K with $I \trianglelefteq \mathcal{O}_K$. $\mathcal{O}_K$ is a Dedekind Domain, so we can factor I into a unique product of prime power ideals. Essentially, we have $I = \mathfrak{p}_i^{\alpha_i} \cdots \mathfrak{p}_k^{\alpha_k}$ meaning $I \cong \bigoplus_{i=1}^{k} \mathfrak{p}_i^{\alpha_i}$ for prime ideals $\mathfrak{p}_i$. Then we can factor the quotient ring seeing $\mathcal{O}_K/I \cong \bigoplus_{i=1}^{k} \mathcal{O}_K/\mathfrak{p}_i^{\alpha_i}$ using the generalized Chinese Remainder Theorem. With these ideas, we seek to prove that we have a chain $X^{N(I)^m} \equiv \cdots \equiv X^{N(I)^{a-1}} \pmod{I}$ where N is the ideal norm and $m, a \in \mathbb{Z}$. Before we can do this, we need to prove that there are chains for prime power ideals of $\mathcal{O}_K$ like we did for $\mathbb{Z}$.

Lemma 10. *Let $\mathcal{O}_K$ be as defined above and $\mathfrak{p}^\alpha \trianglelefteq \mathcal{O}_K$ for $\alpha \in \mathbb{Z}$ where $\mathfrak{p}$ is a nonzero prime ideal of $\mathcal{O}_K$. Then $\mathcal{O}_K/\mathfrak{p}^\alpha$ exhibits a chain $\forall X \in \mathcal{O}_K/\mathfrak{p}^\alpha$.*

Proof. Note that $\mathcal{O}_K/\mathfrak{p}^\alpha$ has q^α elements where $q = N(\mathfrak{p})$, and that $\varphi(\mathfrak{p}^\alpha) = q^{\alpha-1}(q-1)$. We need to show that $X^{q^{\alpha m}} - X^{q^{\alpha(m-1)}} \equiv 0 \pmod{\mathfrak{p}^\alpha}$, but note that it suffices to prove that $X^{q^{\alpha+\beta}} - X^{q^{\alpha+\beta-1}} \equiv 0 \pmod{\mathfrak{p}^\alpha}$ using an arbitrary $\beta \in \mathbb{Z}$. Let $\mathfrak{X}$ be the ideal generated by $X \in \mathcal{O}_K/\mathfrak{p}^\alpha$. Combining these ideas, suppose $\mathfrak{X}$ and $\mathfrak{p}^\alpha$ are coprime. Using Euler's Theorem, we see

$$X^{q^{\alpha+\beta}} - X^{q^{\alpha+\beta-1}} \equiv X^{q^{\alpha+\beta-1}}(X^{q^{\alpha+\beta-1}(q-1)} - 1) \tag{1}$$

$$\equiv X^{q^{\alpha+\beta-1}}(X^{q^\beta \varphi(\mathfrak{p}^\alpha)} - 1) \tag{2}$$

$$\equiv 0 \pmod{\mathfrak{p}^\alpha} \tag{3}$$

for $\beta \in \mathbb{Z}$. Now when $\mathfrak{X}$ and $\mathfrak{p}^\alpha$ are not coprime, we must have $\mathfrak{X} \subseteq \mathfrak{p}^\beta \subseteq \mathfrak{p}$ for $\beta \leq \alpha$. Since $\mathcal{O}_K$ is a Dedekind Domain, to contain is to divide, meaning we have $\mathfrak{p} \mid \mathfrak{X}$ and $X \in \mathfrak{p}$. Moreover since $q^{\alpha+\beta-1} \geq \alpha$, such X satisfies $X^{q^{\alpha+\beta-1}} \equiv 0 \pmod{\mathfrak{p}^\alpha}$ so we can conclude that $X^{q^{\alpha+\beta}} \equiv X^{q^{\alpha+\beta-1}} \pmod{\mathfrak{p}^\alpha}$ and since the β value is arbitary, we have a chain from $X^{q^{\alpha m}}$ down to $X^{q^{\alpha-1}}$ modulo $\mathfrak{p}^\alpha$ for some $m \in \mathbb{Z}$. □

Now that we have this result generalized, a generalization of **Theorem 9** follows neatly to conclude the proofs for this paper.

Theorem 11. *Let $\mathcal{O}_K$ be as defined above and $I = \mathfrak{n} \trianglelefteq \mathcal{O}_K$ with $\mathfrak{n} = \mathfrak{p}_1^{\alpha_1} \cdots \mathfrak{p}_k^{\alpha_k}$ for nonzero prime ideal $\mathfrak{p}_i$ and $\alpha_i \in \mathbb{Z}$. Then we have a chain*

$$X^{N(\mathfrak{n})^m} \equiv \ldots \equiv X^{N(\mathfrak{n})^{a-1}} \pmod{\mathfrak{n}} \; \forall X \in \mathcal{O}_K/I$$

$$\iff$$

$$(N(\mathfrak{p}_i) - 1) \mid (N(\mathfrak{n})/N(\mathfrak{p}_i))^a - N(\mathfrak{n})/N(\mathfrak{p}_i))^{a-1})$$

for $m, a \in \mathbb{Z}^+$

Proof. Recall that since $\mathcal{O}_K$ is a Dedekind Domain, we can write $\mathcal{O}_K/I \cong \bigoplus_{i=1}^{k} \mathcal{O}_K/\mathfrak{p}_i^{\alpha_i}$ meaning it suffices to verify the result for $\mathcal{O}_K/\mathfrak{p}_i^{\alpha_i}$ for an arbitary $\mathfrak{p}_i^{\alpha_i} \mid \mathfrak{n}$. We've seen in **Lemma 10** that when $\mathfrak{X} = (X)$ and $\mathfrak{p}_i^{\alpha_i}$ are not coprime, we have a chain, so we will forgo that case. Now let $q_i^{\alpha_i} = N(\mathfrak{p}_i^{\alpha})$, and suppose $\mathfrak{X}$ and $\mathfrak{p}_i^{\alpha_i}$ are coprime, and that $\mathcal{O}_K/I$ exhibits a chain. Using the ideal factorization of $\mathfrak{n}$, we look at $X^{N(\mathfrak{n})^a} \equiv X^{N(\mathfrak{n})^{a-1}} \pmod{\mathfrak{p}_i^{\alpha_i}}$. We have

$$X^{N(\mathfrak{n})^a} \equiv X^{N(\mathfrak{n})^{a-1}} \pmod{\mathfrak{n}} \tag{1}$$

$$\iff (X^{(N(\mathfrak{n})/q_i^{\alpha_i})^a})^{q_i^{\alpha_i - 1}} \equiv (X^{(N(\mathfrak{n})/q_i^{\alpha_i})^{a-1}})^{q_i^{\alpha_i - 1}} \pmod{\mathfrak{p}_i^{\alpha_i}} \tag{2}$$

Using inverses of X, we now get

$$X^{q_i^{\alpha_i - 1}((N(\mathfrak{n})/q_i^{\alpha_i})^a - (N(\mathfrak{n})/q_i^{\alpha_i})^{a-1}} \equiv 1 \pmod{\mathfrak{p}_i^{\alpha_i}} \tag{3}$$

$$\iff \varphi(\mathfrak{p}_i^{\alpha_i}) \mid q_i^{\alpha_i - 1}((N(\mathfrak{n})/q_i^{\alpha_i})^a - (N(\mathfrak{n})/q_i^{\alpha_i})^{a-1}) \tag{4}$$

Upon expanding $\varphi(\mathfrak{p}_i^{\alpha_i})$, we see

$$\frac{q_i^{\alpha_i - 1}((N(\mathfrak{n})/q_i^{\alpha_i})^a - (N(\mathfrak{n})/q_i^{\alpha_i})^{a-1})}{\varphi(\mathfrak{p}_i^{\alpha_i})} \tag{5}$$

$$= \frac{q_i^{\alpha_i - 1}((N(\mathfrak{n})/q_i^{\alpha_i})^a - (N(\mathfrak{n})/q_i^{\alpha_i})^{a-1})}{q_i^{\alpha_i - 1}(q_i - 1)} \tag{6}$$

$$= \frac{((N(\mathfrak{n})/q_i^{\alpha_i})^a - (N(\mathfrak{n})/q_i^{\alpha_i})^{a-1})}{q_i - 1} \in \mathbb{Z} \tag{7}$$

and note that $q_i = N(\mathfrak{p})$ as stated earlier so we have arrived at the necessary conclusion of $(N(\mathfrak{p}_i) - 1) \mid (N(\mathfrak{n})/N(\mathfrak{p}_i))^a - N(\mathfrak{n})/N(\mathfrak{p}_i))^{a-1})$ if and only if there exists a chain modulo $\mathfrak{n}$. □

Now let's look at some examples and non-examples of quotient rings that satisfy the properties in **Theorem 11**.

Example 1: Let $\mathcal{O}_K = \mathbb{Z}[\sqrt{-2}]$ with $\mathfrak{n} = (3) = (1 + \sqrt{-2})(1 - \sqrt{-2})$ and $a = 2$. Since both prime ideals have the same norm, we only need to complete one computation. We have $(9/3)^2 - (9/3) = 9 - 3 = 6$ and $(3 - 1) \mid 6$ so $\mathbb{Z}[\sqrt{-2}]/(3)$ exhibits a chain for $a > 1$.

Example 2: Let $\mathcal{O}_K$ be any ring of integers of a number field K with $\mathfrak{n}$ as a nonzero prime ideal. We have $\mathcal{O}_K/\mathfrak{n}$ exhibits a chain for $a > 0$.

Proof. Note that $\mathcal{O}_K/\mathfrak{n}$ is a field of order $N(\mathfrak{n}) = q$ where q is a prime power. Since we have $\mathcal{O}_K/\mathfrak{n}$ as a field, $X^q \equiv X \pmod{\mathfrak{n}} \forall X \in \mathcal{O}_K/\mathfrak{n}$ meaning $X^{N(\mathfrak{n})^m} \equiv (X^{q^{m-1}})^q \equiv X^{q^{m-1}} \pmod{\mathfrak{n}}$, and we have a chain from X^{q^m} down to X modulo $\mathfrak{n}$ as desired. □

Non-example 1: Let $\mathcal{O}_K = \mathbb{Z}[i]$ with $\mathfrak{n} = (3+i) = (1+i)(2-i)$ and $a = 2$. The computation with $\mathfrak{p} = (1+i)$ is trivial since $N(1+i) = 2$ so let $\mathfrak{p} = (2-i)$. We have $(10/5)^2 - (10/5) = 2$ and $(5-1) = 4 \nmid 2$ so there is no chain for all $X \in \mathbb{Z}[i]/(3+i)$ when $a = 2$, but note that when $a > 2$ we have a chain.

Non-Example 2: Let $\mathcal{O}_K = \mathbb{Z}[i]$ with $\mathfrak{n} = (5+5i) = (1+i)(2-i)(2+i)$ and $a = 2$. Once again, the first computation is trivial, but we also have the $N(2-i) = N(2+i)$ so we only need to complete one computation. We see $(50/5)^2 - (50/5) = 90$ and $4 \nmid 90$ so there is no chain for all $X \in \mathbb{Z}[i]/(5+5i)$, but once again, if $a > 2$, we would have a chain.

Conclusion

Vanishing polynomials are already a highly explored idea, but the establishing of this polynomial as vanishing exhibits an interesting chain which could prove helpful in modular exponentiation tasks. Practically, knowing such a chain exists might not be very useful, but in computations it could be. Moreover, while illustrating the chain of congruences, we find relationships between prime numbers that determine the existence of a chain modulo n. One could possibly argue that the divisibility relationship amongst such primes could be more interesting than the chain, which is just one example of how important prime numbers are in mathematics.

While we've established the chain and found the neat relationships between prime numbers that facilitate these chains, there is still more to find on this topic. For example, do there exist infinitely many n with this chain? This is the same question as determining whether there are infinitely many primes satisfying the divisibility properties in **Theorem 9** or **Theorem 11**. I conjecture there are infinitely many n, but naturally proving that there are infinitely many primes of some form is extremely hard and requires more time and effort. Another hard question could be possible closed forms for the primes involved in constructing a chain rather than divisibility requirements. These few questions are rather interesting and require research papers themselves. I encourage the reader to think about these puzzling questions as they continue their mathematical careers.

References

[1] **Andrews, G.E.** (1994). *Number Theory.* Dover Publications.

[2] **Pinter, C.C.** (1990). *A Book of Abstract Algebra.* New York: McGraw-Hill.

[3] **Neukirch, J.** (1999). *Algebraic Number Theory.* Springer-Verlag.

[4] **Milne, J.S.** (2020). *Algebraic Number Theory* (v3.08). Found at `https://www.jmilne.org/math/CourseNotes/ANT.pdf`.

[5] **I. Niven and D. Warren.** (1957). *A generalization of Fermat's Theorem*, Proc. Amer. Math. Soc. 8, pp.306–313.

[6] **Robert Gilmer** (1999). *The Ideal of Polynomials Vanishing on a Commutative Ring*. Amer. Math. Soc. Vol. 127, No. 5, pp. 1265-1267.