โครงการ

การเรียนการสอนเพื่อเสริมประสบการณ์

ชื่อโครงการ พหุนามอินเตอร์เซกทีฟในรูปแบบ
$(x^3 - n)(x^2 + 3^t)$ และ $(x^3 - n)(x^2 + 3m^2)$
Intersective polynomials of the forms
$(x^3 - n)(x^2 + 3^t)$ and $(x^3 - n)(x^2 + 3m^2)$

ชื่อนิสิต นาย วชิรวิทย์ ไชยฟองศรี 5933542523

ภาควิชา คณิตศาสตร์และวิทยาการคอมพิวเตอร์
สาขาวิชา คณิตศาสตร์

ปีการศึกษา 2562

คณะวิทยาศาสตร์ จุฬาลงกรณ์มหาวิทยาลัย

พหุนามอินเตอร์เซกทีฟในรูปแบบ $(x^3 - n)(x^2 + 3^t)$ และ $(x^3 - n)(x^2 + 3m^2)$

นาย วชิรวิทย์ ไชยฟองศรี เลขประจำตัว 5933542523

โครงงานนี้เป็นส่วนหนึ่งของการศึกษาตามหลักสูตรวิทยาศาสตรบัณฑิต
สาขาวิชาคณิตศาสตร์ ภาควิชาคณิตศาสตร์และวิทยาการคอมพิวเตอร์
คณะวิทยาศาสตร์ จุฬาลงกรณ์มหาวิทยาลัย
ปีการศึกษา 2562

Intersective polynomials of the forms $(x^3 - n)(x^2 + 3^t)$ and $(x^3 - n)(x^2 + 3m^2)$

Mr. Wachirawit Chaifongsri

A Project Submitted in Partial Fulfillment of the Requirements
for the Degree of Bachelor of Science Program in Mathematics
Department of Mathematics and Computer Science
Faculty of Science Chulalongkorn University
Academic Year 2019

หัวข้อโครงงาน	พหุนามอินเตอร์เซกทีฟในรูปแบบ $(x^3-n)(x^2+3^t)$ และ $(x^3-n)(x^2+3m^2)$
โดย	นาย วชิรวิทย์ ไชยฟองศรี
สาขาวิชา	คณิตศาสตร์
อาจารย์ที่ปรึกษาโครงงานหลัก	ศาสตราจารย์ ดร. ยศนันต์ มีมาก

ภาควิชาคณิตศาสตร์และวิทยาการคอมพิวเตอร์ คณะวิทยาศาสตร์ จุฬาลงกรณ์มหาวิทยาลัย อนุมัติให้นับโครงงานฉบับนี้เป็นส่วนหนึ่ง ของการศึกษาตามหลักสูตรปริญญาบัณฑิต ในรายวิชา 2301499 โครงงานวิทยาศาสตร์ (Senior Project)

. . . . . หัวหน้าภาควิชาคณิตศาสตร์
และวิทยาการคอมพิวเตอร์

(ศาสตราจารย์ ดร.กฤษณะ เนียมมณี)

คณะกรรมการสอบโครงงาน

. . . . . อาจารย์ที่ปรึกษาโครงงานหลัก

(ศาสตราจารย์ ดร. ยศนันต์ มีมาก)

. . . . . กรรมการ

(ศาสตราจารย์ ดร.พัฒนี อุดมกะวานิช)

. . . . . กรรมการ

(ผู้ช่วยศาสตราจารย์ ดร.ธีรพงษ์ พงษ์พัฒนเจริญ)

วชิรวิทย์ ไชยฟองศรี: พหุนามอินเตอร์เซกทีฟในรูปแบบ $(x^3 - n)(x^2 + 3^t)$ และ $(x^3 - n)(x^2 + 3m^2)$. (INTERSECTIVE POLYNOMIALS OF THE FORMS $(x^3-n)(x^2+3^t)$ AND $(x^3-n)(x^2+3m^2)$)
อ.ที่ปรึกษาโครงงานหลัก: ศาสตราจารย์ ดร. ยศนันต์ มีมาก, 23 หน้า.

กำหนดให้ $f(x)$ เป็นพหุนามโมนิกที่มีสัมประสิทธิ์เป็นจำนวนเต็ม เรากล่าวว่า $f(x)$ มีสมบัติ *อินเตอร์เซกทีฟ* ก็ต่อเมื่อ $f(x)$ ไม่มีรากคำตอบที่เป็นจำนวนเต็ม แต่ มีรากคำตอบบนมอดุโล m สำหรับจำนวนนับ m ในการทำโครงงานครั้งนี้ เราได้ศึกษาพหุนามที่มีสมบัติอินเตอร์เซกทีฟในรูปแบบ $(x^3-n)(x^2 + 3^t)$ และ $(x^3 - n)(x^2 + 3m^2)$ เมื่อ n เป็นจำนวนนับที่ไม่สามารถหารด้วยกำลังสามของจำนวนเต็มลงตัว t เป็นจำนวนนับคี่ และ m เป็นจำนวนเต็ม

ภาควิชา คณิตศาสตร์และวิทยาการคอมพิวเตอร์ ลายมือชื่อนิสิต วชิรวิทย์ ไชยฟองศรี
สาขาวิชา . คณิตศาสตร์ . ลายมือชื่อ อ.ที่ปรึกษาโครงงานหลัก ยศนันต์ มีมาก
ปีการศึกษา . . . . 2562 . . . .

5933542523 : MAJOR MATHEMATICS. WACHIRAWIT CHAIFONGSRI: INTERSECTIVE POLYNOMIALS OF THE FORMS $(x^3 - n)(x^2 + 3^t)$ AND $(x^3 - n)(x^2 + 3m^2)$.
ADVISOR: PROFESSOR DR. YOTSANAN MEEMARK, Ph.D., 23 pp.

Let $f(x)$ be a monic polynomial with integer coefficients. We say that $f(x)$ is *intersective* if $f(x)$ does not have an integer root but do have a root modulo m for all $m \in \mathbb{N}$. In this work, we study intersective polynomials of the form $(x^3 - n)(x^2 + 3^t)$ and $(x^3 - n)(x^2 + 3m^2)$ where n is a cubic free positive integer, t odd and m is an integer.

Department . Mathematics and Computer Science . Student's Signature Wachirawit Chaifongsri
Field of Study . . Mathematics . . Advisor's Signature . . Yotsanan Meemark . .
Academic Year . . . . . 2019 . . . . .

Acknowledgements

I would like to express my special thanks of gratitude to my advisor, Professor Yotsanan Meemark, Ph.D. who gives me an opportunity to do this project. It also helps me in doing a lot of research and I come to know about so many new things I am really thankful to them. Also, I would like to express my thanks to project committee: Professor Patanee Udomkavanich, Ph.D. and Assistant Professor Teeraphong Phongpattanachareon , Ph.D. for their great suggestions and comments. Finally, I would like to thank my parents and friends who helps me a lot in finalizing this project within the limited time frame.

Wachirawit Chaifongsri

Contents

Chapter 1
Preliminaries

1.1 Background

Let $f(x)$ be a polynomial with integer coefficients. We say that $f(x)$ is *intersective* if $f(x)$ does not have any integer root but do have a root modulo m for all $m \in \mathbb{N}$. This kind of polynomial provides a counterexample to the local-global principle. Namely, there exists a polynomial in $\mathbb{Z}[x]$ which has a root locally modulo m for all $m \in \mathbb{N}$ but does not have a globally root in $\mathbb{Z}$. It follows Brandl et al. [2] that $f(x)$ cannot be irreducible over $\mathbb{Q}$ since in this case there must be a prime p for which $f(x) \equiv 0 \pmod{p}$ is insolvable. Consequently, an intersective polynomial has at least two irreducible factors over $\mathbb{Q}$. Hyde et al. [3] gave a characterization for a cubic free n such that $(x^3 - n)(x^2 + 3)$ is an intersective polynomial by using only elementary number-theoretic techniques available in undergraduate course. Their main result is as follows.

Theorem 1. Let n be a cubic free integer. Then $f(x) = (x^3 - n)(x^2 + 3)$ is intersective if and only if n is congruent to $9k + 1$ and every prime factor of n is congruent to 1 modulo 3.

We next discuss some of Hyde's tools. Let p be an odd prime, a, b and c be integers, and $\left(\frac{*}{p}\right)$ be the *Legendre symbol* defined by

$$\left(\frac{a}{p}\right) = \begin{cases} 1, & \text{if } p \nmid a, \text{ and } x^2 \equiv a \pmod{p} \text{ is solvable,} \\ -1, & \text{if } p \nmid a, \text{ and } x^2 \equiv a \pmod{p} \text{ is insolvable,} \\ 0, & \text{if } p \mid a. \end{cases}$$

To determine the Legendre symbol, we usually use:

Proposition 2. (Quadratic reciprocity law) If p and q are distinct positive odd primes, then

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}}.$$

Proposition 3. Let p be a positive odd prime. Then

$$\left(\frac{-3}{p}\right) = \begin{cases} 1, & \text{if } p \equiv 1 \pmod 3, \\ -1, & \text{if } p \equiv 2 \pmod 3, \\ 0, & \text{if } p = 3. \end{cases}$$

Proof. Let p be a positive odd prime. If $p = 3$, then $\left(\frac{-3}{p}\right) = 0$. Now we assume that $p \neq 3$. By Proposition 2

$$\left(\frac{-3}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{3}{p}\right) = (-1)^{\frac{p-1}{2}} \cdot \left(\frac{p}{3}\right)(-1)^{\frac{p-1}{2}} = \left(\frac{p}{3}\right).$$

Then $\left(\frac{p}{3}\right) = 1$ if $p \equiv 1 \pmod 3$ and $\left(\frac{p}{3}\right) = -1$ if $p \equiv 2 \pmod 3$. □

Let m and n be positive integers and a an integer such that $\gcd(a, m) = 1$. We say that a is an *$n-$th power residue* m if the congruence $x^n \equiv a \pmod m$ is solvable. To determine if a is an n-th power residue modulo m, we use the next elementary proposition in basic number theory.

Proposition 4. Suppose m is a number having primitive roots and let $a \in \mathbb{Z}$ be such that $\gcd(a, m) = 1$ and $n \in \mathbb{N}$. Then a is an n-th power residue of m if and only if $a^{\frac{\phi(m)}{d}} \equiv 1 \pmod m$ where $d = \gcd(n, \phi(m))$.

Finally, to lift our solutions modulo p^j to solution modulo p^{j+1} where $j \in \mathbb{N}$ and p is a prime, we must use the following Hensel's lemma.

Lemma 5. (Hensel's Lemma) Let $f(x) \in \mathbb{Z}[x]$. Let p be a prime and let r be a solution of the congruence $f(x) \equiv 0 \pmod p$. If p does not divide $f'(r)$, then the congruence $f(x) \equiv 0 \pmod{p^k}$ is solvable for all $k \in \mathbb{N}$.

We also need another refined version of Hensel's lemma presented with proof as follows.

Lemma 6. (Refined Hensel's Lemma) Let $f(x) \in \mathbb{Z}[x]$ and $j \in \mathbb{N}$. Suppose that there is an $a \in \mathbb{Z}$ such that $f(a) \equiv 0 \pmod{p^j}$, $p^\tau \| f'(a)$ and $j \geq 2\tau+1$. If $b \equiv a \pmod{p^{j-\tau}}$, then $f(b) \equiv f(a) \pmod{p^j}$ and $p^\tau \| f'(b)$. Moreover, there is a unique t modulo p such that $f(a+tp^{j-t}) \equiv 0 \pmod{p^{j+1}}$. Therefore, $f(x) \equiv 0 \pmod{p^k}$ is solvable for all $k \in \mathbb{N}$.

Proof. We begin with the Taylor's expansion of $f(b)$

$$f(b) = f(a+tp^{j-\tau}) \equiv f(a) + tp^{j-\tau}f'(a) \pmod{p^{2j-2\tau}}.$$

Here the modulus is divisible by p^{j+1}, because $2j-2\tau = j+(j-2\tau) \geq j+1$. Hence,

$$f(a+tp^{j-\tau}) \equiv f(a) + tp^{j-\tau}f'(a) \pmod{p^{j+1}}.$$

Since both terms on the right hand side are divisible by p^j, the term on the left side is divisible by p^j. When we divide through by p^j we find

$$\frac{f(a+tp^{j-\tau})}{p^j} \equiv \frac{f(a)}{p^j} + t\frac{p^{j-\tau}f'(a)}{p^j} \equiv \frac{f(a)}{p^j} + t\frac{f'(a)}{p^\tau} \pmod{p}.$$

Since the coefficient t is relatively prime to p so there is a unique t modulo p for which the right side is divisible by p. To finish the proof, we note that $f'(x)$ is a polynomial with integer coefficients so that

$$f'(a+tp^{j-\tau}) \equiv f'(a) \pmod{p^{j-\tau}}$$

for any integer t. But $j-\tau \geq \tau+1$, so this congruence holds modulo $p^{\tau+1}$. Since p^τ exactly divides $f'(a)$, we conclude that p^τ exactly divides $f'(a+tp^{j-\tau})$. □

1.2 Objective

Hyde et al. [2] gave an infinitely family of polynomials that are intersective and used only techniques available in an undergraduate course in number theory. Hence, we are interesting in intersective polynomials of the form $(x^3-n)(x^2+3^t)$ and $(x^3-n)(x^2+3m^2)$ where t and m are positive integers.

In the next chapter, we provides some lemmas in order to prove our main results in Section 2.1 and present our main results in Section 2.2. We find necessary and sufficient conditions for intersective polynomials of these forms. This allows us to determine two infinite families of intersective polynomials.

Chapter 2
Main Results

In this chapter, we present our main results on intersective polynomials. We study polynomials of the form $(x^3-n)(x^2+3^t)$ and $(x^3-n)(x^2+3m^2)$ where n is a cubic free positive integer and t and m are positive integers. We obtain a characterization of n such that these polynomials are intersective similar to Hyde's. We begin with some lemmas in the first section and we prove our main theorems in the later section.

2.1 Some lemmas

We collect some lemmas that will be repeatedly used in the proof of our main results in this section. We also list some remarks in the following two lemmas. Their proofs are elementary.

Lemma 7. Let n be a positive integer and let p be a prime. If every prime factor of n is congruent to 1 modulo p, then $n \equiv 1 \pmod{p}$.

Proof. Assume that every prime factor of n is congruent to 1 modulo p. Let $p_1, p_2, \ldots, p_t$ be the prime factors of n. Then for each $i \in \{1, 2, ..., t\}$, $p_i = 1 + k_i p$ for some integer k_i. Thus,

$$n = \prod_{i=1}^{t} (1 + k_i p)^{a_i} \equiv 1 \pmod{p}$$

for some $a_1, a_2, \ldots, a_t \in \mathbb{N}$. □

Lemma 8. Let $g(x), h(x) \in \mathbb{Z}[x]$, and p a prime. If $g(x)h(x)$ is intersective and $g(x) \equiv 0 \pmod{p^k}$ does not have a solution for some $k \in \mathbb{N}$, then $h(x) \equiv 0 \pmod{p^l}$ has a solution for all $l \in \mathbb{N}$.

Proof. Suppose that $g(x) \equiv 0 \pmod{p^k}$ and $h(x) \equiv 0 \pmod{p^l}$ are insolvable for some $k, l \in \mathbb{N}$. Since $g(x)h(x)$ is intersective, so $g(x)h(x) \equiv 0 \pmod{p^{k+l}}$ must have a solution, say w. By the assumption, $p^k \nmid g(w)$ and $p^l \nmid h(w)$, so $p^{k+l} \nmid g(w)h(w)$, a contradiction. □

2.2 Intersective polynomials

In this section, we will prove our main results which are similar to Hyde's. We remark that the Chinese remainder theorem allows us to work only on the existence of solutions modulo every prime power instead.

Theorem 9. Let n be a cubic free integer greater than 1 and t an odd positive integer. Then the polynomial $f(x) = (x^3 - n)(x^2 + 3^t)$ is intersective if and only if $n \equiv 1 \pmod{9}$ and every prime factor of n is congruent to 1 modulo 3.

Proof. Assume that $n \equiv 1 \pmod{9}$ and every prime factor of n is congruent to 1 modulo 3. Let p be a prime. We consider three cases : $p \equiv 1 \pmod{3}$, $p \equiv 2 \pmod{3}$ and $p = 3$, respectively.

Case 1. $p \equiv 1 \pmod{3}$. So the Legendre symbol $\left(\frac{-3}{p}\right)$ is 1. Since t is an odd positive integer, we have $\left(\frac{-3^t}{p}\right) = \left(\frac{3^{t-1}}{p}\right)\left(\frac{-3}{p}\right) = 1$. It follows that the congruence $x^2 + 3^t \equiv 0 \pmod{p}$ has a solution, say u. Since $p \nmid 3$, $p \nmid u$. Therefore, $p \nmid 2u$ and $2u = g'(u)$ where $g(x) = x^2 + 3^t$. By Hensel's lemma, $x^2 + 3^t \equiv 0 \pmod{p^k}$ has a solution for all $k \in \mathbb{N}$.

Case 2. $p \equiv 2 \pmod{3}$. Since every prime factor of n is congruent to 1 modulo 3, $p \nmid n$, so $n^{p-1} \equiv 1 \pmod{p}$ by Fermat's little theorem. By Proposition 4, the congruence $x^3 - n \equiv 0 \pmod{p}$ has a solution, say v. Since $p \nmid n$, $p \nmid v$. Also $p \nmid 3$, so $p \nmid 3v^2$ and $3v^2$ is the derivative of $x^3 - n$ at $x = v$. By Hensel's lemma, $x^3 - n \equiv 0 \pmod{p^k}$ has a solution for all $k \in \mathbb{N}$.

Case 3. $p = 3$. Since $n \equiv 1 \pmod{9}$, we have $n \equiv 1, 10, 27 \pmod{3^3}$. Note that $1^3 \equiv 1, 4^3 \equiv 10, 7^3 \equiv 19$ modulo 3^3, so $x^3 \equiv n \pmod{3^3}$ is solvable. Moreover, the derivative of $x^3 - n$, which is $3x^2$, evaluated at $1, 4$, and 7 equals $3, 12$, and 21, respectively and is divisible by 3 and not divisble by other powers of 3 in all cases.

So we apply the refined Hensel's lemma with $j = 3, \tau = 1$, and conclude that $x^3 - n \equiv 0 \pmod{3^k}$ is solvable for all $k \in \mathbb{N}$. Then, $f(x) \equiv 0 \pmod{p^j}$ is solvable for all primes p and $j \in \mathbb{N}$.

Hence, by th Chinese remainder theorem, $f(x) \equiv 0 \pmod{m}$ is solvable for each $m \in \mathbb{N}$. This establishes the intersective property of $f(x)$.

Conversely, suppose that $f(x) = (x^3 - n)(x^2 + 3^t)$ is intersective. Let p be a prime such that $p \mid n$. We will prove that $f(x)$ cannot be intersective when $p \equiv 2 \pmod{3}$ and $p = 3$. So, we can conclude that $p \equiv 1 \pmod{3}$.

Case 1. $p \equiv 2 \pmod{3}$ We show that $x^2 + 3^t \equiv 0 \pmod{p^c}$ is insolvable for some $c \in \mathbb{N}$. Since t is an odd positive integer, $t = 2s + 1$ for some $s \in \mathbb{N} \cup \{0\}$. Then $3^t = 3^{2s+1} \equiv 3 \pmod{2^3}$. Note that all squares modulo 8 are $0, 1$ and 4. Thus, $x^2 + 3^t \equiv 0 \pmod{2^3}$ does not have a solution. Next, we assume that $p \neq 2$. So $\left(\frac{-3}{p}\right) = -1$. Since t is an odd positive integer, we have $\left(\frac{-3^t}{p}\right) = -1$, so $x^2 + 3^t \equiv 0 \pmod{p}$ does not have a solution. Hence, $x^2 + 3^t \equiv 0 \pmod{p^c}$ is insolvable for some $c \in \mathbb{N}$. By Lemma 8, $x^3 - n \equiv 0 \pmod{p^k}$ has a solution for all $k \in \mathbb{N}$, so $x^3 - n \equiv 0 \pmod{p^3}$ has a solution, say v. Since $p \mid n$, we have $p \mid v$. It follows that $p \mid v^3$, and so $p^3 \mid n$ which contradicts n is a cubic free integer.

Case 2. $p = 3$. Suppose that $x^2 + 3^t \equiv 0 \pmod{3^{t+1}}$ has a solution, say w. Then $3^t \mid w^2$, so $w^2 = h \cdot 3^t$ for some $h \in \mathbb{N}$. Since $3 \mid w$, we let $w = 3^a M$ for some $a, M \in \mathbb{N}$ and $3 \nmid M$. Then $w^2 = 3^{2a} M^2$. Since $3 \nmid M$, $2a$ is the highest power of 3 that divides w^2. We will show that $3 \mid h$. If $3 \nmid h$, then t is the highest power of 3 that divides w^2, so $t = 2a$ which is impossible where t is an odd positive integer. Thus, $3 \mid h$. Since $w^2 = h \cdot 3^t$, $3^{t+1} \mid w^2$. But $3^{t+1} \mid w^2 + 3^t$, so $3^{t+1} \mid 3^t$ which is a contradiction. Hence, $x^2 + 3^t \equiv 0 \pmod{3^{t+1}}$ does not have a solution.

Assume that $x^3 - n \equiv 0 \pmod{3^k}$ does not have a solutions for some $k \in \mathbb{N}$. It follows by Lemma 8 that $f(x) = (x^3 - n)(x^2 + 3^t) \equiv 0 \pmod{3^{k+t+1}}$ does not have a solutions which is a contradiction because $f(x)$ is intersective. Thus, $x^3 - n \equiv 0 \pmod{3^k}$ has a solution for all $k \in \mathbb{N}$. So $x^3 - n \equiv 0 \pmod{3^3}$ has a solution, say z. Then $3 \mid z$ because $3 \mid n$, then $3^3 \mid z^3$, i.e. $3^3 \mid n$ which is impossible because n is a cubic free integer.

Thus, every prime factor of n is congruent to 1 modulo 3, by Lemma 7, $n \equiv 1 \pmod 3$. Since $x^2 + 3^t \equiv 0 \pmod{3^{t+1}}$ is insolvable, by Lemma 8, $f(x) = (x^3 - n)(x^2 + 3^t) \equiv 0 \pmod{3^{k+t+1}}$ does not have a solution which contradicts the fact that $f(x)$ is intersective. Thus, $x^3 - n \equiv 0 \pmod{3^k}$ is solvable for all $k \in \mathbb{N}$, so the congruence $x^3 - n \equiv 0 \pmod{3^2}$ must have a solution. Since the cubes modulo 9 are 1 or 8, $n \equiv 1, 8 \pmod 9$. If $n \equiv 8 \pmod 9$, we have $n \equiv 2 \pmod 3$ which contradicts the previous calculation. Hence, $n \equiv 1 \pmod 9$. □

Theorem 10. Let n be a cubic free integer greater than 1 and m an integer. Then the polynomial $f(x) = (x^3 - n)(x^2 + 3m^2)$ is intersective if and only if $n \equiv 1 \pmod 9$ and every prime factor of n is congruent to 1 modulo 3.

Proof. Assume that $n \equiv 1 \pmod 9$ and every prime factor of n is is congruent to 1 modulo 3. Let p be a prime. We consider three cases : $p \equiv 1 \pmod 3$, $p \equiv 2 \pmod 3$ and $p = 3$.

Case 1. $p \equiv 1 \pmod 3$. If $p \nmid m, p \nmid -3m^2$. Then the Legendre symbol $\left(\frac{-3m^2}{p}\right) = 1$. It follows that $x^2 + 3m^2 \equiv 0 \pmod p$ has a soltution, say u. Since $p \nmid 3$, we have $p \nmid u$. Thus, $p \nmid 2u$ and $g'(u) = 2u$ where $g(x) = x^2 + 3m^2$. By Hensel's lemma, $x^2 + 3m^2 \equiv 0 \pmod{p^k}$ has a solution for all $k \in \mathbb{N}$. Next, we assume that $p \mid m$ and write $m = p^r s$ for some $r \in \mathbb{N}, s \in \mathbb{Z}$ and $p \nmid s$. Then $\left(\frac{-3s^2}{p}\right) = 1$, so there is a $z \in \mathbb{Z}$ such that $z^2 + 3s^2 \equiv 0 \pmod p$. Let $x_0 = p^r z$. Then $x_0^2 + 3m^2 = p^{2r}(z^2 + 3s^2) \equiv 0 \pmod{p^{2r+1}}$. Since $p^r \| 2x_0$ and $2x_0$ is the derivative of $x^2 + 3m^2$ at $x = x_0$, by applying the refined Hensel's lemma with $j = 2r + 1$ and $\tau = r$, we can conclude that $x^2 + 3m^2 \equiv 0 \pmod{p^k}$ has a solution for all $k \in \mathbb{N}$.

Case 2. $p \equiv 2 \pmod 3$. Since every prime factor of n is congruent 1 modulo 3, $p \nmid n$, so $n^{p-1} \equiv 1 \pmod p$ by Fermat's little theorem. By Proposition 4, $x^3 - n \equiv 0 \pmod p$ has a solution, say v. Since $p \nmid n$, $p \nmid v$. Also $p \nmid 3$, so $p \nmid 3v^2$, and $3v^2$ is the derivative of $x^3 - n$ at $x = v$. By Hensel's lemma, the $x^3 - n \equiv 0 \pmod{p^k}$ has a solution for all $k \in \mathbb{N}$.

Case 3. $p = 3$. Since $n \equiv 1 \pmod 9$, we have $n \equiv 1, 10, 19 \pmod{3^3}$. Note that $1^3 \equiv 1, 4^3 \equiv 10, 7^3 \equiv 19$ modulo 3^3, so $x^3 \equiv n \pmod{3^3}$ is solvable. Moreover, the derivative of $x^3 - n$, which is $3x^2$, evaluated at $1, 4$, and 7 equals $3, 12$, and 21,

respectively and divisible by 3 and not divisible by other powers of 3 in all cases. So we apply the refined Hensel's lemma with $j = 3$ and $\tau = 1$, we conclude that $x^3 - n \equiv 0 \pmod{3^k}$ is solvable for all $k \in \mathbb{N}$. Then, $f(x) \equiv 0 \pmod{p^j}$ is solvable for all primes p and $j \in \mathbb{N}$.

Hence, by the Chinese remainder theorem, $f(x) \equiv 0 \pmod{m'}$ is solvable for each $m' \in \mathbb{N}$. This establishes the intersective property of $f(x)$.

Conversely, suppose that $f(x) = (x^3 - n)(x^2 + 3m^2)$ is intersective. Let p be a prime such that $p \mid n$. We will prove that $f(x)$ cannot be intersective when $p \equiv 2 \pmod 3$ and $p = 3$. So, we can conclude that $p \equiv 1 \pmod 3$.

Case 1. $p \equiv 2 \pmod 3$. We claim that $x^2 + 3m^2 \equiv 0 \pmod{p^c}$ is insolvable for some $c \in \mathbb{N}$. Let $m = 2^t K$ for some $t \in \mathbb{N} \cup \{0\}$, $K \in \mathbb{N}$ and K odd. Suppose that $x^2 + 3m^2 \equiv 0 \pmod{2^{2t+3}}$ has a solution, say x_1. Then $x_1^2 + 3m^2 \equiv 0 \pmod{2^t}$ and $x_1^2 \equiv 0 \pmod{2^{2t}}$. Let $x_1 = 2^d e$ for some $d, e \in \mathbb{N}$ and e odd. Then $2^{2d}e^2 = x_1^2 \equiv 0 \pmod{2^{2t}}$, so $d \geq t$. Observe that $0 \equiv x_1^2 + 3m^2 = 2^{2d}e^2 + 3 \cdot 2^{2t}K^2 = 2^{2t}((2^{d-t}e)^2 + 3K^2) \pmod{2^{2t+3}}$. Thus, $(2^{d-t}e)^2 + 3K^2 \equiv 0 \pmod 8$. Since K is odd, $K^2 \equiv 1 \pmod 8$, so $0 \equiv (2^{d-t}e^2) + 3K^2 \equiv (2^{d-t}e^2) + 3 \pmod 8$. It follows that $x^2 + 3 \equiv 0 \pmod 8$ is solvable which is impossible because all squares modulo 8 are $0, 1$ and 4.

Now, we assume that $p \neq 2$. Then $\left(\frac{-3}{p}\right) = -1$, so $x^2 + 3 \equiv 0 \pmod p$ is insolvable. If $p \nmid m$, then $\left(\frac{-3m^2}{p}\right) = -1$, so $x^2 + 3m^2 \equiv 0 \pmod p$ is insolvable. Next, we suppose that $p \mid m$ and write $m = p^f i$ for some $f \in \mathbb{N}, i \in \mathbb{Z}$ and $p \nmid i$. Assume that $x^2 + 3m^2 \equiv 0 \pmod{p^{2f+1}}$ has a solution, say x_2. Then $p \mid x_2$, so $x_2 = p^\alpha \beta$ for some $\alpha \in \mathbb{N}, \beta \in \mathbb{Z}$ and $p \nmid \beta$. It follows that $0 \equiv x_0^2 + 3m^2 = p^{2\alpha}\beta^2 + 3p^{2f}i^2 = p^{2f}((p^{\alpha-f}\beta)^2 + 3i^2) \pmod{p^{2f+1}}$, so $(p^{\alpha-f}\beta)^2 + 3i^2 \equiv 0 \pmod p$. Since $p \nmid i, -3$ is a square modulo p which is a contradiction. Hence, we have the claim. By Lemma 8, $x^3 - n \equiv 0 \pmod{p^k}$ is solvable for all $k \in \mathbb{N}$. Also $x^3 - n \equiv 0 \pmod{p^3}$ has a solution, say g. Then $p \mid g$, so $p^3 \mid g^3$. It follows that $p^3 \mid n$ which contradicts n is a cubic free integer.

Case 2. $p = 3$. Let $m = 3^{r_1}s_1$ for some $r_1 \in \mathbb{N} \cup \{0\}, s_1 \in \mathbb{Z}$ and $3 \nmid s_1$. We will claim that $x^2 + 3m^2 \equiv 0 \pmod{3^{2r_1+2}}$ is insolvable. Suppose that $x^2 + 3m^2 \equiv 0 \pmod{3^{2r_1+2}}$

has a solution, say w. Then $3 \mid w, w = 3^{e_1}d_1$ for some $e_1 \in \mathbb{N}, d_1 \in \mathbb{Z}$ and $3 \nmid d_1$. It follows that $0 \equiv w^2+3m^2 = 3^{2e_1}d_1^2+3^{2r_1+1}s_1^2 \equiv 3^{2e_1}d_1^2 \pmod{3^{2r_1+1}}$, so $2r_1+1 \leq 2e_1$. Since $2r_1 + 1$ is odd, $2r_1 + 2 \leq 2e_1$. Thus, $0 \equiv w^2 + 3m^2 = 3^{2e_1}d_1^2 + 3^{2r_1+1}s_1^2 \equiv 3^{2r_1+1}s_1^2 \pmod{3^{2r_1+2}}, s_1^2 \equiv 0 \pmod 3$ which contradicts because $3 \nmid s_1$. Hence, we have the claim. By Lemma 8, $x^3 - n \equiv 0 \pmod{3^k}$ is solvable for all $k \in \mathbb{N}$. Also $x^3 - n \equiv 0 \pmod{3^3}$ has a solution, say g'. Then $3 \mid g'$, so $3^3 \mid (g')^3$. It follows that $3^3 \mid n$ which contradicts n is a cubic free integer.

Therefore, every prime factor of n must be congruent to 1 modulo 3, by Lemma 7, we can conclude that $n \equiv 1 \pmod 3$. Since the cubes modulo 9 are 1 or 8, $n \equiv 1$ or $8 \pmod 9$. If $n \equiv 8 \pmod 9$, we have $n \equiv 2 \pmod 3$ which contradicts the previous calculation. Hence, $n \equiv 1 \pmod 9$. □

Bibliography

[1] D. Berend and Y. Bilu, Polynomials with roots modulo every integer, *Proc. Amer. Math Soc.*, **124** (1996) 1663–1671.

[2] R. Brandl, D. Bubboloni, I. Hupp, Polynomials with roots mod p for all primes p, *J. Group Theory*, **4** (2001) 233–239.

[3] M. Hyde, D. Lee and K. Spearman, Polynomials $(x^3-n)(x^2+3)$ solvable modulo any integer, *Amer. Math. Monthly*, **121** (2014) 355–358.

Appendix

The Project Proposal of Course 2301399 Project Proposal

Academic Year 2019

Project Tittle (Thai)	พหุนามอินเตอร์เซกทีฟในรูปแบบ $(x^3-n)(x^2+3^t)$ และ $(x^3-n)(x^2+3m^2)$
Project Tittle (English)	Intersective polynomials of the forms $(x^3-n)(x^2+3^t)$ and $(x^3-n)(x^2+3m^2)$
Project Advisor	Professor Dr. Yotsanan Meemark
By	Mr. Wachirawit Chaifongsri ID 5933542523 Mathematics, Department of Mathematics and Computer Science, Faculty of Science, Chulalongkorn University

---

Background, Rationale and Scope

A polynomial $f(x)$ in $\mathbb{Z}[x]$ is *intersective* if $f(x)$ does not have an integer root but do have a root modulo m for all positive integers m. Intersective polynomials provide an example of a Van der Corput set [2]. Berend and Bilu [1] gave a criterion to decide if the polynomial $f(x) \in \mathbb{Z}[x]$ has a root modulo every positive integer by using the Galois group of $f(x)$ .They applied their results to show that $f(x) = (x^3-19)(x^2+x+1)$ has a root modulo m for every positive integer m. Their proof involved Galois theory, and some results from algebraic number theory, namely, discriminant and resultant.

Later, Hyde et al. [3] used only Hensel's lemma in elementary number theory to gave a characterization for a cubic free positive integer n such that $(x^3-n)(x^2+3)$

is an intersective polynomial. Their main theorem is as follows.

Theorem. *Let n be a cubic free. Then $f(x) = (x^3 - n)(x^2 + 3)$ is intersective if and only if n is of the form $9k+1$ and every prime factor of n is congruent to 1 modulo 3.*

This provides an infinite family of intersective polynomials.

In this project, we plan to use elementary number theory to determine other infinite families of intersective polynomials. For example, we study the polynomials of the form $(x^3 - n)(x^2 + 3^t)$ and $(x^3 - n)(x^2 + 3m^2)$ where n is a cubic free positive integer and t, m are positive integers. We wish to obtain some characterizations similar to Hyde's.

Objectives

To determine families of intersective polynomials of the forms $(x^3 - n)(x^2 + 3^t)$ and $(x^3 - n)(x^2 + 3m^2)$ where n is a cubic free positive integer and t, m are positive integers.

Project Activities

1. Review some background in number theory on polynomials modulo m.
2. Study intersective polynomials from $[1]$, $[2]$ and $[3]$.
3. Find conditions on n, t and m such that the polynomials $(x^3 - n)(x^2 + 3^t)$ and $(x^3 - n)(x^2 + 3m^2)$ are intersective.
4. Write the report.

Duration

Procedue	August 2019 – April 2020								
	Aug.	Sep.	Oct.	Nov.	Dec.	Jan.	Feb.	Mar.	Apr.
1.Review some background in number theory on polynomials modulo m.									
2.Study intersective polynomials from $[1], [2]$ and $[3]$.									
3.Find conditions on n, t and m such that the polynomials $(x^3 - n)(x^2 + 3^t)$ and $(x^3 - n)(x^2 + 3m^2)$ are intersective.									
4.Write the report.									

Benefits

Obtain some characterizations of n, t and m such that the polynomials $(x^3 - n)(x^2 + 3^t)$ and $(x^3 - n)(x^2 + 3m^2)$ are intersective.

Equipments

1. Computer
2. Paper
3. Printer
4. Stationery

References

[1] D. Berend, Y. Bilu, Polynomials with roots modulo every integer, *Proc. Amer. Math. Soc.* **124** (1996) 1663–1671.

[2] M. Hyde, D. Lee, K. Spearman, Polynomials $(x^3 - n)(x^2 + 3)$ Solvable modulo any integer, *Amer. Math. Monthly* **121** (2014) 355–358.

[3] T. Kamae, M. M. France, Van der Corput's difference theorem, *Isr. J. Math.* **31** (1978) 249–256.

Biography

Wachirawit Chaifongsri ID 5933542523
Department of Mathematics and Computer Science,
Faculty of Science, Chulalongkorn University