Polynomials

Tho Nguyen
tnguyenx@asu.edu

1. Find all polynomials $f, g$ in $\mathbb{C}[X]$ such that $f^3 - g^2$ is a nonzero constant.

Solution

If $f$ or $g$ is a constant then both $f, g$ are constant.

Now assume that $\deg(f), \deg(g) > 0$ and $f^3 - g^2 = a \in \mathbb{C}^*$. Let $b = a^{1/3}$ then we have $g^2 = f^3 - b^3 = (f - b)(f^2 + bf + b^2)$.

If $f - b$ and $f^2 + bf + b^2$ have a common root $x_0$ then we have

$$0 = f(x_0)^2 + bf(x_0) + b^2 = b^2 + b^2 + b^2 = 3b^2$$

, thus $b = 0$ and hence $a = 0$. So $f - b$ and $f^2 + bf + b^2$ are relatively prime. Therefore both $f - b$ and $f^2 + bf + b^2$ are squares of polynomials in $\mathbb{C}[X]$. Now let $f - b = A(x)^2$ and $f^2 + bf + b^2 = B(x)^2$ then

$$B^2 = (A^2 + b)^2 + b(A^2 + b) + b^2 = A^4 + 3bA^2 + 3b^2$$

so

$$B^2 = (A^2 + c)(A^2 + d)$$

where $c = \frac{b(-3 + i\sqrt{3})}{2}$ and $d = \frac{b(-3 - i\sqrt{3})}{2}$.

Again, if $A(x)^2 + c$ and $A(x)^2 + d$ have a common root $x_1$ in $\mathbb{C}$ then $c - d = A(x_1)^2 + c - A(x_1)^2 - d = 0$, so $c = d$, which is not possible. So $A^2 + c$ and $B^2 + c$ are relatively prime in $\mathbb{C}[X]$.

Therefore $A(x)^2 + c = h(x)^2$.

But then $c = (h - A)(h + A)$, thus both $h - A$, $h + A$ are constant, and hence $h, A$ are also constant.

Therefore $f = b + A^2$ is also a constant polynomial, which contradicts to $\deg(f) > 0$.

So $f, g$ are constant polynomials.

2. Find all pairs of polynomials $P(x)$ and $Q(x)$ with real coefficients for which

$$P(x)Q(x + 1) - P(x + 1)Q(x) = 1$$
for all $x \in R$.

**Solution**

Suppose $P, Q$ satisfy

$$P(x)Q(x + 1) - P(x + 1)Q(x) = 1$$

Then none of $P, Q$ can be 0 and $P, Q$ have no common non constant factors.

We have

$$P(x + 1)Q(x) - P(x + 1)Q(x) = P(x - 1)Q(x) - P(x)Q(x - 1) = 1$$

Thus

$$P(x)(Q(x + 1) - Q(x - 1)) = Q(x)(P(x + 1) + P(x - 1))$$

Because $P, Q$ have no non constant factors, we have $P(x)|P(x + 1) + P(x - 1)$.

This implies that $P(x + 1) + P(x - 1) = 2P(x)$.

So

$$P(x + 1) - P(x) = P(x) - P(x - 1)$$

Let $H(x) = P(x + 1) - P(x)$ then $H(x) = H(x - 1)$, thus $H$ is a constant polynomial.

Therefore $P(x) - P(x - 1) = a \in \mathbb{R}$. Therefore $P(x) = ax + b$.

Similarly, $Q(x) = cx + d$.

Then

$$P(x)Q(x + 1) - P(x + 1)Q(x) = bc - ad$$

So $1 = bc - ad$.

Therefore $P(x) = ax + b$ and $Q(x) = cx + d$ with $bc - ad = 1$.

3. Prove that every prime number is a divisor of the polynomial

$$x^6 - 11x^4 + 36x^2 - 36$$

which does not have rational roots.

**Solution** Let $P(x) = x^6 - 11x^4 + 36x^2 - 36$ then $P(x) = (x^2-2)(x^2-3)(x^2-6)$.

So $P$ has no rational roots.

Let $p$ be a prime number greater than 3.

If $\left(\frac{2}{p}\right) = 1$ or $\left(\frac{3}{p}\right) = 1$ then $p|P(x)$, else we have $\left(\frac{6}{p}\right) = 1$.

4. Find the number of pairs of polynomials $P(x), Q(x) \in \mathbb{R}[X]$ such that

$$P(x)^2 + Q(x)^2 = x^{2n} + 1$$
and \( \deg(P) > \deg(Q) \).

**Solution** Because \( \deg(P) > \deg(Q) \), we have the leading coefficient of \( P \) is \( \pm 1 \).

Now assume that the leading coefficient of \( P \) is 1, then we have

\[
(P + iQ)(P - iQ) = \prod_{k=0}^{n-1} (x + e^{\frac{i(2k+1)\pi}{2n}}) \cdot \prod_{k=0}^{n-1} (x - e^{\frac{i(2k+1)\pi}{2n}})
\]

\( P + iQ \) is a polynomial of degree \( n \), in order for \( P, Q \) to have real coefficients, then for each \( k \) in \( \{0, 1, ..., n-1\} \), exactly one of \( x + e^{\frac{i(2k+1)\pi}{2n}} \) or \( x - e^{\frac{i(2k+1)\pi}{2n}} \) is a factor of \( P + iQ \). Thus there are \( 2^n \) pairs of \( P, Q \) with the leading coefficient of \( P \) is 1.

If the leading coefficient of \( P \) is \(-1 \), we have \( 2^n \) pairs of \( P, Q \). Therefore, there are \( 2^{n+1} \) pairs of \( P, Q \) satisfying the hypothesis.

5. Let \( f \) be a non constant polynomial with positive integer coefficients. Prove that if \( n \) is a positive integer, then \( f(n) \) divides \( f(f(n)+1) \) if and only if \( n = 1 \).

**Solution** Let \( f(x) = a_0 + a_1x + ... + a_dx^d \) with \( a_0, ..., a_d \in \mathbb{Z}^+ \). We have

\[
f(f(n)+1) = a_0 + a_1(1+f(n)) + ... + a_d(1+f(n))^d \equiv a_0 + ... + a_d \equiv f(1) \mod f(n)
\]

If \( n = 1 \) then of course \( f(f(n)+1) \equiv 0 \mod f(n) \).

If \( n > 1 \) then \( f(1) < f(n) \) because \( a_0, ..., a_d \in \mathbb{Z}^+ \), therefore \( f(f(n)+1) \not\equiv 0 \mod f(n) \).

6. Let \( p \) be a prime number. Let \( h(x) \) be a polynomial with integer coefficients such that \( h(0), h(1), ..., h(p^2-1) \) are distinct modulo \( p^2 \). Prove that \( h(0), h(1), ..., h(p^3-1) \) are distinct modulo \( p^3 \).

**Solution** We use Taylor’s theorem:

\[
h(x + y) = h(x) + h'(x)y + \frac{h''(x)}{2!}y^2 + ... + \frac{h^{(n)}(x)}{n!}y^n
\]

Here \( h'(x), ..., \frac{h^{(n)}(x)}{n!} \in \mathbb{Z}[X] \).

For \( x = 0, 1, ..., p - 1 \), we have

\[
h(x + p) \equiv h(x) + ph'(x) \mod p^2
\]

Since \( h'(x) \in \mathbb{Z}[x] \), we have \( h'(x + mp) \equiv h'(x) \mod p \) for every \( m \in \mathbb{Z} \).

Therefore, \( h'(x) \not\equiv 0 \mod p \) for all \( x \in \mathbb{Z} \).

Now for \( x = 0, 1, ..., p^2-1 \) and \( y = 0, 1, ..., p - 1 \) we have

\[
h(x + yp^2) \equiv h(x) + p^2yh'(x) \mod p^3
\]
Thus $h(x), h(x + p^2), \ldots, h(x + (p - 1)p^2)$ run over all of the residue classes modulo $p^3$ congruent to $h(x)$ modulo $p^2$. Because $h(x)$ covers all the residue classes modulo $p^3$, $h(0), \ldots, h(p^3 - 1)$ are distinct modulo $p^3$.

7. Let

$$P_n(x) = 1 + 2x + 3x^2 + \ldots + nx^{n-1}$$

Prove that $P_n$ and $P_m$ are relatively prime for every $n \neq m$.

**Solution**

**Lemma 1** Let

$$f(x) = a_0 + a_1x + \ldots + a_nx^n$$

be a polynomial with $0 < a_0 \leq a_1 \ldots \leq a_n$ then let $z$ be a complex root of $f$ then $|z| \leq 1$.

**Proof** Let $f(z) = 0$ then from $(z - 1)f(z) = 0$, we have

$$a_nz^{n+1} = (a_n - a_{n-1})z^n + \ldots + (a_1 - a_0)z + a_0$$

If $|z| > 1$ then $|a_nz^{n+1}| \leq (|a_n - a_{n-1}| + \ldots + |a_1 - a_0| + |a_0|)|z|^n = |a_n||z|^n$, contradiction.

Therefore, $|z| \leq 1$.

**Lemma 2**

Let $f(x) = a_0 + a_1x + \ldots + a_nx^n$ be a polynomial with positive coefficients then for every root $z \in \mathbb{C}$ of $f$ satisfies $r \leq |z| \leq R$, for

$$r = \min\left\{\frac{a_0}{a_1}, \ldots, \frac{a_{n-1}}{a_n}\right\}$$

$$R = \max\left\{\frac{a_0}{a_1}, \ldots, \frac{a_{n-1}}{a_n}\right\}$$

**Proof** Apply lemma 1 to polynomial $f\left(\frac{z}{R}\right)$, we have $|z| \leq R$. Apply lemma 1 to the reverse of polynomial $f\left(\frac{z}{r}\right)$, we have $|z| \geq r$.

Suppose that $P_m(z) = P_n(z)$ for some $z \in \mathbb{C}$ and $0 < m < n \in \mathbb{Z}^+$. we cannot have $n = m + 1$ because $P_{m+1} - P_m = (m + 1)z^{m+1}$.

Thus $n - m \geq 2$.

Apply lemma 2 to $P_m$ we have $|z| \leq 1 - \frac{1}{m}$.

Apply lemma 2 to $\frac{P_n(x) - P_m(x)}{x^{n-m}}$, we have $|z| \geq 1 - \frac{1}{m+2}$.

So $1 - \frac{1}{m} \geq 1 - \frac{1}{m+2}$, contradiction.

8. Prove that for every $n$ then $7^n + 1$ has at least (not necessarily distinct) $2n + 3$ prime factors.

**Solution** We prove by induction on $n$. 

4
For \( n = 0 \), then \( 7^7 + 1 = 8 \) has 3 prime factors.
Assume that \( 7^n + 1 \) has at least \( 2n + 3 \) prime factors.
Let \( x = 7^n \) then
\[
\frac{x^7 + 1}{x + 1} = \frac{(x + 1)^7 - ((x + 1)^7 - x^7 - 1)}{x + 1}
= (x + 1)^6 - \frac{7x^6 + 21x^5 + 35x^4 + 35x^3 + 21x^2 + 7x}{x + 1}
= (x + 1)^6 - \frac{7x(x + 1)(x^2 + x + 1)^2}{x + 1}
= (x + 1)^6 - 7^{n+1}(x^2 + x + 1)^2
= ((x + 1)^3 - 7^m(x^2 + x + 1))( (x + 1)^3 + 7^m(x^2 + x + 1))
\]
where \( m = \frac{1 + 7^n}{2} \in \mathbb{Z}^+ \).
Now
\[
(x + 1)^3 - 7^m(x^2 + x + 1) = x^2(x - 7^m) + x(3x - 7^m) + 3x + 1 - 7^m
> x^2 + x > 2
\]
So \((x + 1)^3 - 7^m(x^2 + x + 1)\) has at least 1 prime factor and \((x + 1)^3 + 7^m(x^2 + x + 1)\) has at least 1 prime factor.
By induction hypothesis then \( x + 1 \) has at least \( 2n + 3 \) prime factors. Therefore, \( 7^{n+1} + 1 \) has at least \( 2n + 3 + 2 = 2(n + 1) + 3 \) prime factors.

9. Find all pairs of positive integers \((m, n)\) such that
\[
(x^2 + x + 1)^m | (x + 1)^n - x^n - 1
\]

**Solution**

**Lemma** \( x^2 + x + 1 | (x + 1)^k - x^k \) if and only if \( k \equiv 0 \mod 6 \)

**Proof.** If \( k \equiv 0 \mod 6 \) then let \( k = 6m \) with \( m \in \mathbb{Z}^+ \)
\[
(x + 1)^{6m} - x^{6m} = (x^2 + 2x + 1)^3m - (x^3)^{2m}
\equiv x^{3m} - 1^n \mod x^2 + x + 1
\equiv 1 - 1 \equiv 0 \mod x^2 + x + 1
\]
If \( k \not\equiv 0 \mod 6 \) then just consider \( k = 6m + r \) with \( r = 1, 2, \ldots, 5 \) we see that \( x^2 + x + 1 \nmid (x + 1)^{6m+r} - x^{6m+r} \).

Now let \( f(x) = (x + 1)^n - x^n - 1 \).
If \( m = 1 \), then \( x^2 + x + 1 | (x + 1)^n - x^n - 1 \), this is equivalent to \( 6 | n \pm 1 \).
If \( m = 2 \), then \((x^2 + x + 1)^2|f(x)\), thus \( x^2 + x + 1|f'(x) = n((x + 1)^{n-1} - x^{n-1})\). By the lemma then \(6|n - 1\). When \(6|n - 1\) then \(x^2 + x + 1|f(x)\) by the case \(m = 1\).

If \( m > 2 \) then \((x^2 + x + 1)^3|f(x)\), thus \( x^2 + x + 1|f''(x) = n(n - 1)((x + 1)^{n-2} - x^{n-2})\) and \( x^2 + x + 1|f'(x) = n((x + 1)^{n-1} - x^{n-1})\).

By the lemma then \(6|n - 2\) and \(6|n - 1\), a contradiction. Therefore, all pairs of \((m, n)\) such that \((x^2 + x + 1)^m|(x + 1)^n - x^n - 1\) are \((1, 6k \pm 1), (2, 6k)\) with \(k \in \mathbb{Z}^+\).

10. Let \(a\) be a perfect square. Assume that \(7 + a\) has \(d\) prime divisors (not necessarily distinct). Show that \(7^m + a^m\) has at least \(2n + d\) prime divisors (not necessarily distinct).

Solution Just prove by induction on \(n\).

Let \(7^m = x\) and \(a^m = y\) then

\[
\frac{x^7 + y^7}{x + y} = \frac{(x + y)^7 - ((x + y)^7 - x^7 - y^7)}{x + y}
\]

\[
= (x + y)^6 - 7xy(x^2 + xy + y^2)^2
\]

Let \(a = m^2\) then \(y = b^2\) with \(b = m^n\) then \(7xy = (7^{\frac{n+1}{2}}b)^2 = c^2\).

So

\[
x^7 + y^7 = (x + y)((x + y)^3 - c(x^2 + xy + y^2))((x + y)^3 + c(x^2 + xy + y^2))
\]

We have

\[
(x+y)^3+c(x^2+xy+y^2) > (x+y)^3-c(x^2+xy+y^2) = (x+y)^3-\sqrt{7xy}(x^2+xy+y^2) > 1
\]

Indeed, we show that

\[
(x + y)^3 - \sqrt{7xy}(x^2 + xy + y^2) > 1
\]

11. Find the minimum of the function

\[
F(m, n) = (m + n)^3 - \sqrt{7mn}(m^2 + mn + n^2)
\]

where \(m, n \in \mathbb{Z}^+\) and \(m \neq n\).

Solution Assume \(m > n\) then \(F(m, n) \geq F(n + 1, n) \geq F(2, 1) = 27 - 5\sqrt{14}\)

12. Find all monic polynomial \(P(x)\) with integer coefficients such that there exists a positive integer \(n\) satisfying

\[
P(x)^2|(x + 1)^n - x^n - 1
\]
Solution
If $P(x)$ is a constant then $P(x) = 1$ because $P(x)$ is monic.
Assume now that $P(x)$ has a positive degree.
Let $f(x) = (x + 1)^n - x^n - 1$.
Let $\alpha$ be a complex root of $P(x)$ then $\alpha$ is a common root of $f(x)$ and $f'(x)$.
Thus
\[(\alpha + 1)^{n-1} - \alpha^{n-1} = (\alpha + 1)^n - \alpha^n - 1 = 0\]
But then
\[(\alpha + 1)^n - \alpha^n = (\alpha + 1)(\alpha + 1)^{n-1} - \alpha^n - 1
= (\alpha^n + \alpha^{n-1}) - \alpha^n - 1
= \alpha^{n-1} - 1\]
So
\[(\alpha + 1)^{n-1} = \alpha^{n-1} = 1\]
Thus
\[|\alpha| = |\alpha + 1| = 1\]
Let $\alpha = a + ib$ with $a, b \in \mathbb{R}$ and $a^2 + b^2 = 1$.
Then from $|\alpha + 1| = 1$, we have
\[(a + 1)^2 + b^2 = 1 = a^2 + b^2\]
so $a = -\frac{1}{2}$ and $b = \pm\frac{\sqrt{3}}{2}$.
Therefore if $\alpha$ is a root of $P(x)$ then $\alpha = \frac{-1 \pm \sqrt{3}}{2}$.
The minimal polynomial of $\frac{-1 \pm \sqrt{3}}{2}$ over $\mathbb{Q}$ is $x^2 + x + 1$, and $P(x)$ is a monic polynomial, we have
\[P(x) = (x^2 + x + 1)^m\]
for some $m \in \mathbb{Z}^+$.
Now from $\alpha$ is a root of $x^3 - 1 = (x - 1)(x^2 + x + 1)$ and $\alpha^{n-1} = 1$, we have
\[x^3 - 1 | x^{n-1} - 1\]
Hence $3|n - 1$.
If $n = 6m + 1$ then $x^2 + x + 1 | (x + 1)^n - x^n - 1$ and $x^2 + x + 1 | (x + 1)^{n-1} - x^{n-1}$.
If $n = 6m + 4$ then $x^2 + x + 1 \nmid (x + 1)^{n-1} - x^{n-1}$.
Therefore, $6|n - 1$.
In this case, if $m > 2$ then $x^2 + x + 1 | f^{(3)}(x) = n(n-1)((x + 1)^{n-2} - x^{n-2})$,
which is not possible when $6|n - 1$.
Therefore, $P(x) = x^2 + x + 1$. 

13. Find all pairs of positive integers \((m, n)\) such that there exists a monic polynomial \(P(x)\) with integer coefficients satisfying
\[
P(x)^m | (x + 1)^n - x^n - 1
\]
**Solution** For \(m = 1\), just take \(P(x) = (x + 1)^n - x^n - 1\) for every \(n \in \mathbb{Z}^+\).
For \(m > 1\), using arguing as the Problem 8, we have \(m = 2\), \(P(x) = x^2 + x + 1\) and \(n = 6k + 1\) with \(k \in \mathbb{Z}\).

14. Let \(n \in \mathbb{Z}^+\), find \(\gcd((x + 1)^n - x^n, (x + 1)^{n^2+1} - x^{n^2+1} - 1)\) in \(\mathbb{Q}[x]\)
**Solution.**
Let \(P(x) = \gcd((x + 1)^n - x^n, (x + 1)^{n^2+1} - x^{n^2+1} - 1)\).
If \(P(x)\) is not a constant polynomial, then let \(\alpha\) be a root of \(P(x)\).
Then
\[
(\alpha + 1)^n = \alpha^n
\]
and
\[
(\alpha + 1)^{n^2+1} - \alpha^{n^2+1} - 1 = 0
\]
But then
\[
(\alpha + 1)^{n^2+1} - \alpha^{n^2+1} - 1 = (\alpha + 1)((\alpha + 1)^n)^n - \alpha^{n^2+1} - 1
\]
\[
= (\alpha + 1)(\alpha^n)^n - \alpha^{n^2+1} - 1
\]
\[
= \alpha^{n^2} - 1
\]
So
\[
\alpha^{n^2} = 1
\]
Therefore \(|\alpha| = 1\), hence \(|\alpha + 1|^n = |\alpha|^n = 1\).
So
\[
|\alpha + 1| = |\alpha| = 1
\]
Write \(\alpha = a + ib\) with \(a, b \in \mathbb{R}\) then
\[
\alpha = \frac{-1 \pm \sqrt{3}}{2}
\]
So \(P(x) = (x^2 + x + 1)^k\) for \(k \in \mathbb{Z}^+\).
We know that
\[
x^2 + x + 1 | (x + 1)^n - x^n \iff 6 | n
\]
and \(x^2 + x + 1 \nmid (x + 1)^{n-1} - x^{n-1}\) if \(x^2 + x + 1 | (x + 1)^n - x^n\).
Therefore
\[
\gcd((x + 1)^n - x^n, (x + 1)^{n^2+1} - x^{n^2+1} - 1) = 1\text{ if } 6 \nmid n
\]
\[
= x^2 + x + 1\text{ if } 6 | n
\]
15. Let $m, n \in \mathbb{Z}^+$ such that $n|m - 1$. Find $\gcd((x + 1)^n - x^n, (x + 1)^m - x^m - 1)$.

Solution As above, if $6|n$ then $x^2 + x + 1$ is the gcd.
If $6 \nmid n$ then the gcd is 1.