Quadratics

Lecture 8

Justin Stevens

Outline

Method of Undetermined Coefficients

Example. Find the constants a, b, c such that

$$6x^5 + x^4 - 10x^3 + 4x - 1 = \left(2x^3 + 3x^2 - 1\right)\left(ax^2 + bx + c\right).$$

Solution. The only way to produce an x^5 term on the RHS is in the product $(2x^3)(ax^2) = 2ax^5$. This must equal $6x^5$, therefore $a = \mathbf{3}$. The x^4 terms on the RHS are $(2x^3)(bx)$ and $(3x^2)(ax^2)$, so

$$2bx^4 + 3ax^4 = 1x^4 \implies b = \mathbf{-4}.$$

To find c, we compare the constant terms to see $-1 = -1 \cdot c$, so $c = \mathbf{1}$. We can verify that

$$6x^5 + x^4 - 10x^3 + 4x - 1 = \left(2x^3 + 3x^2 - 1\right)\left(3x^2 - 4x + 1\right). \qquad \square$$

Polynomial Division Theorems

Theorem. To divide $n(x)$ by $d(x)$, there exists unique $q(x)$ and $r(x)$:

$$n(x) = d(x)q(x) + r(x), \quad \deg(r) < \deg(d) \text{ or } r(x) = 0.$$

If $r(x) = 0$, then we say $n(x)$ is divisible by $d(x)$.

Theorem. (Factor Theorem) $f(x)$ has a factor of $x - a$ iff $f(a) = 0$.

Definition. If $f(r) = 0$, then r is called a **root** of the polynomial $f(x)$.

Factoring a Cubic

Example. Factor the polynomial $f(x) = x^3 + 11x^2 - 49x - 539$.

Solution. Substituting small values into this expression, we see

$$f(0) = -539, \quad f(1) = -576, \quad f(2) = -585, \quad f(3) = -560, \quad f(4) = -495.$$

Observe that $f(0), f(2)$, and $f(4)$ are all odd. If x is an even integer, then $x^3, 11x^2, -49x$ are all even, while -539 is odd, hence $f(x)$ is odd. Similarly, since $3 \nmid -539$ and $5 \nmid -539$, $f(x)$ cannot have a root divisible by 3 nor 5.

For $x = 7$, $f(7) = 7^3 + 11 \cdot 7^2 - 49 \cdot 7 - 539 = 0$, so $x - 7$ is a factor.

To divide, we use synthetic division:

7	1	11	−49	−539
		7	126	539
	1	18	77	0

Hence $f(x) = (x - 7)(x^2 + 18x + 77)$. Since $7 \cdot 11 = 77$ and $7 + 11 = 18$,

$$f(x) = \boxed{(x - 7)(x + 7)(x + 11)}.$$

Integer Roots

Theorem. Suppose k is a nonzero integer root of the polynomial f with integer coefficients:

$$f(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_2 x^2 + a_1 x + a_0.$$

Then, k must divide the constant coefficient, a_0.

Proof.

Substituting $x = k$ into the polynomial, we see that

$$f(k) = a_n k^n + a_{n-1} k^{n-1} + \cdots + a_2 k^2 + a_1 k + a_0 = 0.$$

Isolating for a_0, $a_0 = -k\left(a_n k^{n-1} + \cdots + a_2 k + a_1\right)$, so $k \mid a_0$. □

A more difficult cubic

Example. Factor the polynomial $f(x) = 24x^3 - 38x^2 - 51x - 10$.

Solution. Since none of $\pm 1, \pm 2, \pm 5$, and ± 10 are roots, the cubic has no integer roots. Therefore, for relatively prime integers s and t, we try s/t:

$$f(\frac{s}{t}) = 24\left(\frac{s}{t}\right)^3 - 38\left(\frac{s}{t}\right)^2 - 51\left(\frac{s}{t}\right) - 10 = 0.$$

Multiplying by t^3 gives $24s^3 - 38s^2t - 51st^2 - 10t^3 = 0$. Isolating for s^3,

$$24s^3 = 38s^2t + 51st^2 + 10t^3 = t\left(38s^2 + 51st + 10t^2\right).$$

Therefore, $24s^3/t$ is an integer. Since $\gcd(s, t) = 1$, $t \mid 24$. Similarly, $s \mid 10$.

Trying cases, we see $-1/4$ is a root:

$-1/4$	24	-38	-51	-10
		-6	11	10
	24	-44	-40	0

A more difficult cubic

Example. Factor the polynomial $f(x) = 24x^3 - 38x^2 - 51x - 10$.

Therefore, $24x^3 - 38x^2 - 51x - 10 = (x + 1/4)\left(24x^2 - 44x - 40\right)$.
Factoring the quadratic by taking out a factor of 4 and searching for roots,

$$24x^2 - 44x - 40 = 4\left(6x^2 - 11x - 10\right) = 4\,(3x + 2)\,(2x - 5)\,.$$

We factor the constants out of each linear factor so the coefficients are 1:

$$\begin{aligned} 24x^3 - 38x^2 - 51x - 10 &= 4\,(x + 1/4)\,(3x + 2)\,(2x - 5) \\ &= 24\left(x + \frac{1}{4}\right)\left(x + \frac{2}{3}\right)\left(x - \frac{5}{2}\right). \end{aligned}$$

We see that the roots are $-1/4, -2/3$, and $5/2$.

Rational Root Theorem

Theorem. A degree n polynomial f with roots $r_1, r_2, \cdots, r_n$ can be factored as

$$f(x) = a_n (x - r_1)(x - r_2) \cdots (x - r_n).$$

Theorem. (Rational Root Theorem) Suppose s/t is a nonzero rational root of

$$f(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0,$$

where the coefficients are integers. Then, $s \mid a_0$ and $t \mid a_n$.

Prime Generating Polynomials

Theorem. Prove that there is no nonconstant polynomial with integral coeficients that produces primes for every integer n.

Proof by Contradiction.

Suppose there is such a polynomial with integer coefficients and $a_k \neq 0$:

$$f(n) = a_k n^k + a_{n-1} k^{n-1} + \cdots + a_2 n^2 + a_1 n + a_0.$$

For a fixed value of n_0, let $f(n_0) = p$ be a prime number. Then, consider

$$\begin{aligned} f(n_0 + tp) &= a_k (n_0 + tp)^k + a_{k-1} (n_0 + tp)^{k-1} + \cdots + a_1 (n_0 + tp) + a_0 \\ &\equiv a_k n_0^k + a_{k-1} n^{k-1} + \cdots + a_1 n_0 + a_0 \\ &\equiv f(n_0) \equiv 0 \pmod{p}. \end{aligned}$$

Since f always generates primes, $f(n_0 + tp) = p$ for all integers t. However, then the polynomial $g(n) = f(n) - p$ has infinite roots, contradiction. $\square$

History of Prime Producing Polynomials

Euler discovered that the polynomial $n^2 + n + 41$ generates 40 consecutive primes for $0 \leq n \leq 39$. However, for $n = 40$, $40^2 + 40 + 41 = 41^2$. In fact, for the first 100 integer values of n, it produces 86 primes.

While there is no prime-producing polynomial, in 1947, it was proved that there exists a positive real number r such that $\lfloor r^{3^n} \rfloor$ is prime for all natural numbers n. The value r is known as **Mills' constant** and its value is unknown, however, assuming the Riemann hypothesis, $r \approx 1.306378\ldots$

Outline

Integers

The set of **integers** are $Z = \{\cdots, -3, -2, -1, 0, 1, 2, 3, \cdots\}$. Properties of addition $(+)$ and multiplication $(\cdot)$ for integers a and b include:

- **Closure:** $a + b$ and $a \cdot b$ are both integers.
- **Associativity:** $a + (b + c) = (a + b) + c$ and $a \cdot (b \cdot c) = (a \cdot b) \cdot c$.
- **Commutativity:** $a + b = b + a$ and $a \cdot b = b \cdot a$.
- **Identity:** $a + 0 = a$ and $a \cdot 1 = a$.
- **Distributivity:** $a \cdot (b + c) = a \cdot b + a \cdot c$ and $(a + b) \cdot c = a \cdot c + b \cdot c$.
- **Additive Inverse:** $a + (-a) = 0$.

These properties imply the integers are a commutative ring.

Positive integers are $\mathbb{Z}^+ = \{1, 2, 3, \cdots\}$. The additive inverses of the positive integers are the **negative integers**. The natural numbers, $\mathbb{N}$, consist of zero combined with the positive integers.

The integers are equipped with an ordering relation; we say a is less than b, denoted $a < b$, if $b - a$ is positive. Then $\min(a, b) = a$ and $\max(a, b) = b$.

Well-Ordering Principle

Theorem. Every non-empty subset of $\mathbb{Z}^+$ has a least element.

Definition. $x \in S$ denotes "x belongs to set S".

Example. Show that there is no integer between 0 and 1.

Proof by Contradiction.

Assume for the sake of contradiction that $S = \{c \in \mathbb{Z} \mid 0 < c < 1\}$, the set of integers between 0 and 1, is non-empty. Hence, S must have a smallest element, say m. However, we see that $m^2 \in \mathbb{Z}$ from closure over multiplication and $0 < m^2 < m < 1$. This contradicts the minimality of m, hence $S = \emptyset$ and there are no integers between 0 and 1. $\square$

Induction

Theorem. Suppose we have a statement P that we wish to show is true for all positive integers at least 1. We can prove this in two steps:

- **Base Case:** Show $P(1)$.
- **Inductive Step:** Show $P(k)$ implies $P(k+1)$ for any integer $k \geq 1$.

The assumption we make is known as the induction hypothesis.

Proof by Contradiction.

Assume that $S = \{n \mid P(n) \text{ is false}\}$ is non-empty. Let the least element of S be m. Observe that $1 \notin S$, therefore $m > 1$. Also by minimality, $m - 1 \notin S$. However by the inductive step, $P(m-1)$ implies $P(m)$, contradiction. $\square$

Max and Min

Example. Prove that $\min(a, b) + \max(a, b) = a + b$.

Proof.

We have two cases to consider. If $a \leq b$, then we have $\min(a, b) = a$ and $\max(a, b) = b$. Otherwise, if $b < a$, then $\min(a, b) = b$ and $\max(a, b) = a$. Either way, the result holds. $\square$

For two positive integers a and b, we write out their prime factorizations:

$$a = p_1^{a_1} p_2^{a_2} \cdots p_k^{a_k}, \quad b = p_1^{b_1} p_2^{b_2} \cdots p_k^{b_k}.$$

Then,

$$\gcd(a, b) = p_1^{\min(a_1, b_1)} p_2^{\min(a_2, b_2)} \cdots p_k^{\min(a_k, b_k)}$$
$$\operatorname{lcm}[a, b] = p_1^{\max(a_1, b_1)} p_2^{\max(a_2, b_2)} \cdots p_k^{\max(a_k, b_k)}.$$

Therefore, $\gcd(a, b) \operatorname{lcm}[a, b] = ab$.

p-adic Valuation

Let a positive integer $n > 1$ be written as $n = p_1^{e_1} p_2^{e_2} \cdots p_k^{e_k}$.

Definition. For each prime, the ***p*-adic valuation** of n is $v_{p_i}(n) = e_i$.

If $\mathbb{P}$ is the set of primes, then another way to write the factorization is

$$n = \prod_{p \in \mathbb{P}} p^{v_p(n)}.$$

Using the law of exponents, we can see the two following theorem.

Theorem. $v_p(mn) = v_p(m) + v_p(n)$ and $v_p(n^c) = cv_p(n)$.

USAMO Problem

Example. (USAMO) Prove that for integers a, b, c,

$$\frac{[a,b,c]^2}{[a,b][b,c][c,a]} = \frac{(a,b,c)^2}{(a,b)(b,c)(c,a)}.$$

Solution. Consider a prime p dividing at least one of a, b, c. Let $v_p(a) = \alpha, v_p(b) = \beta$, and $v_p(c) = \gamma$. WLOG $\alpha \geq \beta \geq \gamma$. Then,

$$v_p\left(\frac{[a,b,c]^2}{[a,b][b,c][c,a]}\right) = 2v_p([a,b,c]) - v_p([a,b]) - v_p([b,c]) - v_p([c,a])$$
$$= 2\alpha - \alpha - \beta - \alpha = -\beta.$$

Furthermore, the number of factors of p on the right hand side is

$$v_p\left(\frac{(a,b,c)^2}{(a,b)(b,c)(c,a)}\right) = 2v_p\left((a,b,c)\right) - v_p\left((a,b)\right) - v_p\left((b,c)\right) - v_p\left((c,a)\right)$$
$$= 2\gamma - \beta - \gamma - \gamma = -\beta.$$

By the Fundamental Theorem of Arithmetic, the two sides are equal.

Rational and Irrational Numbers

A **rational number** can be expressed in the form a/b where a and b are integers and $b \neq 0$. The rationals, $\mathbb{Q}$, are a field since all non-zero elements have a multiplicative inverse. They can be formally defined as an equivalence class of pairs of integers (a, b) with $b \neq 0$ and equivalence relation $(a_1, b_1) \sim (a_2, b_2)$ if and only if $a_1 b_2 = a_2 b_1$.

An **irrational number** cannot be expressed as the ratio of two integers.

A **real number** is a quantity on an infinitely long number line. The reals, $\mathbb{R}$, consist of all rational and irrational numbers, therefore $\mathbb{N} \subset \mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R}$. Notice that $R \subset S$ denotes "R is a subset of S".

Rational and Irrational Numbers

Example. Prove that $\sqrt{2}$ is irrational.

Solution. Assume that $\sqrt{2} = a/b$ for integers a and b. Then,

$$\sqrt{2} = \frac{a}{b} \implies a^2 = 2b^2.$$

We take the 2-adic valuation of both sides of the equation:

$$v_2\left(a^2\right) = 2v_2(a)$$
$$v_2\left(b^2\right) = 2v_2(b) + 1.$$

Therefore, $2v_2(a) = 2v_2(b) + 1$, contradiction. Hence $\sqrt{2}$ is irrational.

Pythagoras and Irrational Numbers

Around 500 BC, Pythagoras founded a religion called Pythagoreanism. The followers thought numbers explained everything in life, from nature to music. Furthermore, they believed every number in the universe was rational.

According to legend, Hippasus was a Pythagorean who was an excellent mathematician. While looking at the pentagram, he took the measure of the length of several sides and found the irrational ratio:

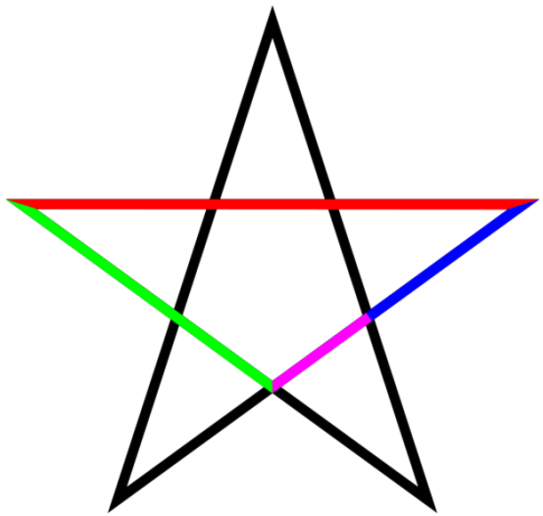

Figure 1: $\frac{\text{red}}{\text{green}} = \frac{\text{green}}{\text{blue}} = \frac{\text{blue}}{\text{purple}} = \frac{1+\sqrt{5}}{2}$

The Golden Ratio

Two quantities are in the **golden ratio** if their ratio is the same of the ratio of their sum to the larger of the two quantities:

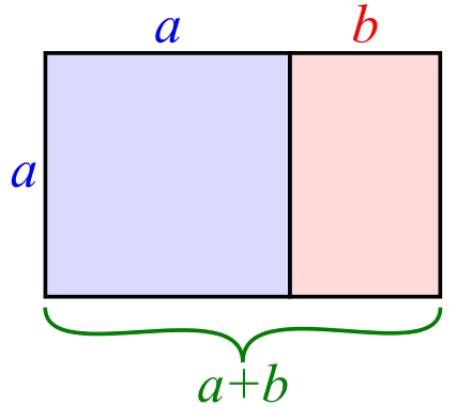

Figure 2: $\frac{a+b}{a} = \frac{a}{b} \stackrel{\text{def}}{=} \varphi$.

Letting $\varphi = \frac{a}{b}$ in the equation above, we see

$$1 + \frac{1}{\varphi} = \varphi \implies \varphi^2 - \varphi - 1 = 0.$$

Using the quadratic formula, $\varphi = \frac{1+\sqrt{5}}{2}$. The other root is $\psi = \frac{1-\sqrt{5}}{2}$.

Binet's Formula

Theorem. (Binet's Formula) The n^{th} Fibonacci number is given by

$$F_n = \frac{\varphi^n - \psi^n}{\sqrt{5}}.$$

Proof. Note $F_1 = (\varphi - \psi)/\sqrt{5} = 1$ and $F_2 = (\varphi^2 - \psi^2)/\sqrt{5} = 1$. Assume the result for $n = k-2$ and $n = k-1$. We then show $n = k$. Observe that φ and ψ are the roots of the quadratic $x^2 - x - 1 = 0$. Hence,

$$\varphi^k = \varphi^{k-1} + \varphi^{k-2}, \quad \psi^k = \psi^{k-1} + \psi^{k-2}.$$

From the definition of Fibonacci numbers and the induction hypothesis

$$\begin{aligned} F_k = F_{k-1} + F_{k-2} &= \frac{\varphi^{k-1} - \psi^{k-1}}{\sqrt{5}} + \frac{\varphi^{k-2} - \psi^{k-2}}{\sqrt{5}} \\ &= \frac{\varphi^k - \psi^k}{\sqrt{5}}. \end{aligned}$$

This is the desired formula for k, hence Binet's Formula is proven.

Golden Spiral

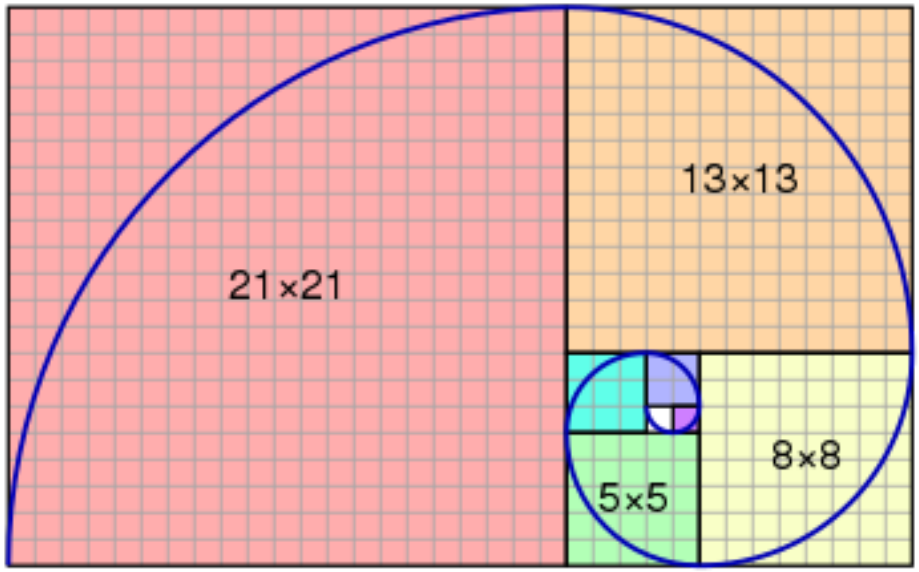

Figure 3: The Golden Ratio Spiral

Outline

Perfect Squares

Definition. Perfect squares are of the form m^2 where m is an integer. Note that n is a perfect square if and only if for all primes p, $v_p(n)$ is even.

Theorem. For coprime a and b, if $ab = c^2$, then a and b are both perfect squares.

Proof.

Let p be an arbitrary prime divisor of c. Taking the p-adic valuation:

$$v_p(a) + v_p(b) = v_p(c^2) = 2v_p(c).$$

Since a and b share no divisors, one member of $\{v_p(a), v_p(b)\}$ is 0 and the other is $2v_p(c)$. Hence, every exponent in the factorization of a and b is even implying a and b are both perfect squares. $\square$

Quadratic Residues

Definition. We call a a **quadratic residue** mod n if there exists an integer x such that $x^2 \equiv a \pmod{n}$. Otherwise, it is a quadratic nonresidue.

Mod	Quadratic Residues
3	0, 1
4	0,1
5	0, 1, 4
7	0, 1, 2, 4

Table 1: Several Examples of Quadratic Residues

Pythagorean Triplets

Definition. A *Pythagorean triple* is a set of three integers x, y, z such that $x^2 + y^2 = z^2$; the triple is said to be *primitive* if $\gcd(x, y, z) = 1$.

Two famous primitive Pythagorean triples are $3, 4, 5$ and $5, 12, 13$.

Suppose that x, y, z is any Pythagorean triple and $d = \gcd(x, y, z)$. If we write $x = dx_1, y = dy_1, z = dz_1$, then $\gcd(x_1, y_1, z_1) = 1$ and

$$x_1^2 + y_1^2 = \frac{x^2 + y^2}{d^2} = \frac{z^2}{d^2} = z_1^2.$$

Hence x_1, y_1, z_1 form a primitive Pythagorean triple.

For a primitive triple, each pair of the integers x, y, and z must be relatively prime. If it were the case that $\gcd(x, y) = d > 1$, then there exists a prime p such that $p \mid d$. Therefore, $p \mid x$ and $p \mid y$, implying $p \mid (x^2 + y^2)$ or $p \mid z^2$, giving $p \mid z$. This contradicts the primality, hence $d = 1$.

Parity of Pythagorean Triples

Example. If x, y, z is a primitive Pythagorean triple, prove that one of the integers x or y is even, while the other is odd.

Proof.

If x and y are both even, then $2 \mid (x^2 + y^2)$ or $2 \mid z^2$, so that $2 \mid z$. Therefore, x, y, z would not be a primitive triple. If, on the other hand, x and y are both odd, then $x^2 \equiv 1 \pmod 4$ and $y^2 \equiv 1 \pmod 4$, leading to

$$z^2 = x^2 + y^2 \equiv 2 \pmod 4.$$

However, the only quadratic residues mod 4 are 0 and 1, contradiction. $\square$

Generator of Pythagorean Triples

Example. Find all primitive solutions to $x^2 + y^2 = z^2$.

WLOG, assume that x is even, therefore y and z are both odd. Furthermore $z - y$ and $z + y$ are even, say $z - y = 2u$ and $z + y = 2v$. Therefore, dividing by 4 and using difference of squares,

$$\left(\frac{x}{2}\right)^2 = \left(\frac{z-y}{2}\right)\left(\frac{z+y}{2}\right) = uv.$$

Notice that u and v are relatively prime; if $\gcd(u, v) = d > 1$, then $d \mid (u - v)$ and $d \mid (u + v)$, or equivalently $d \mid y$ and $d \mid z$.

Since they multiply to a perfect square, $u = t^2$ and $v = s^2$. Therefore,

$$z = v + u = s^2 + t^2, \quad y = v - u = s^2 - t^2, \quad x^2 = 4vu = 4s^2t^2.$$

Therefore, $(x, y, z) = (2st, s^2 - t^2, s^2 + t^2)$ for $s \not\equiv t \pmod 2$.

Table of Pythagorean Triples

		y	x	z
s	t	$(s^2 - t^2)$	$(2st)$	$(s^2 + t^2)$
2	1	3	4	5
3	2	5	12	13
4	1	15	8	17
4	3	7	24	25
5	2	21	20	29
5	4	9	40	41
6	1	35	12	37
6	5	11	60	61

Table 2: The first several Pythagorean triples

Fermat's Method of Infinite Descent

Example. Find all positive integers solutions to $x^3 + 2y^3 = 4z^3$.

Solution. Let (x, y, z) be the solution with the smallest value of z. Then, since the other terms are even, x must be even, so let $x = 2x_1$:

$$8x_1^3 + 2y^3 = 4z^3 \implies 4x_1^3 + y^3 = 2z^3.$$

Similarly, we see that y must be even, so let $y = 2y_1$:

$$4x_1^3 + 8y_1^3 = 2z^3 \implies 2x_1^3 + 4y_1^3 = z^3.$$

Finally, we see that z must be even, so let $z = 2z_1$:

$$2x_1^3 + 4y_1^3 = 8z_1^3 \implies x_1^3 + 2y_1^3 = 4z_1^3.$$

However, then $(x_1, y_1, z_1) = (x/2, y/2, z/2)$ is a solution with a smaller z.

Fermat's Last Theorem for $n = 4$

Example. Prove that there are no integers x, y, z with $x^4 + y^4 = z^2$.

Assume that $x^4 + y^4 = z^2$ is the solution with smallest z. Therefore, (x^2, y^2, z) is a primitive Pythagorean triple. WLOG, let x^2 be even, so

$$x^2 = 2mn, \quad y^2 = m^2 - n^2, \quad z^2 = m^2 + n^2.$$

From the second equation, $y^2 + n^2 = m^2$, so (y, n, m) is a primitive Pythagorean triple. Since y is odd, n must be even, and we parametrize:

$$n = 2rs, \quad y = r^2 - s^2, \quad m = r^2 + s^2.$$

Furthermore, $x^2 = 2mn = 2\left(r^s + s^2\right) 2rs = 4\left(r^s + s^2\right) rs$.

Since they multiply to a perfect square, $r^2 + s^2$ and rs must be perfect squares. Let $r^2 + s^2 = w^2$, $r = u^2$, and $s = v^2$. Therefore,

$$r^2 + s^2 = w^2 = u^4 + v^4.$$

However, then we have found a smaller solution to our original equation since $z = m^2 + n^2 = w^4 + n^2 > w^4 \gg w$, contradiction.

Outline

Prime Factorizations

Example. Let $P(m)$ denote the greatest prime factor of m. Find all $n > 1$ such that $P(n) = \sqrt{n}$ and $P(n+48) = \sqrt{n+48}$.

Example. Find all primes p such that $16p + 1$ is a perfect cube.

Square Root Factors

Example. Let $P(m)$ denote the greatest prime factor of m. Find all $n > 1$ such that $P(n) = \sqrt{n}$ and $P(n+48) = \sqrt{n+48}$.

Solution. We see that $n = p^2$ and $n + 48 = q^2$ for primes p and q. Then,

$$q^2 - p^2 = (q+p)(q-p) = 48.$$

If $q + p = 24$ and $q - p = 2$, then $(q, p) = \mathbf{(13, 11)}$. For $q + p = 12$ and $q - p = 4$, $(q, p) = (8, 4)$ and for $q + p = 8$ and $q - p = 6$, $(q, p) = (7, 1)$. Neither are prime solutions, hence $n = 11^2 = \boxed{121}$.

Perfect Cube

Example. Find all primes p such that $16p + 1$ is a perfect cube.

Solution. Let $16p + 1 = n^3$ for some integer n. Using difference of cubes,

$$16p = n^3 - 1 = (n-1)\left(n^2 + n + 1\right).$$

Since $n^2 + n + 1$ is odd, we must have $16 \mid n - 1$, therefore $n - 1 = 16k$:

$$p = k\left(n^2 + n + 1\right).$$

Since $n^2 + n + 1 > 1$, we must have $k = 1$, so $n = 17$. We then find

$$p = 17^2 + 17 + 1 = \boxed{307}.$$

Perfect Square Condition

Example. Let n be a positive integer such that $2 + 2\sqrt{28n^2 + 1}$ is an integer. Show that $2 + 2\sqrt{28n^2 + 1}$ is the square of an integer.

Solution. Since 28 is even, the radical must be an odd integer; let $\sqrt{28n^2 + 1} = 2m + 1$ for some integer m. Squaring and rearranging gives

$$28n^2 + 1 = 4m^2 + 4m + 1 \implies 7n^2 = m(m + 1).$$

If 7 divides $m + 1$, we let $m = a^2$ and $m + 1 = 7b^2$ where a and b are relatively prime. Substituting gives

$$a^2 + 1 = 7b^2 \implies a^2 \equiv -1 \pmod 7.$$

However, the quadratic residues mod 7 are $0, 1, 2, 4$, contradiction.

Therefore, 7 must divide m. Let $m = 7a^2$ and $m + 1 = b^2$, so

$$2 + 2\sqrt{28n^2 + 1} = 2 + 2(2m + 1) = 4m + 4 = 4b^2 = (2b)^2,$$

which is a perfect square, as desired.

Exponent Factorizations

Theorem. For all positive integers n,

$$x^n - y^n = (x-y)\left(x^{n-1} + x^{n-2}y^1 + x^{n-3}y^2 + \cdots + y^{n-1}\right).$$

For all **odd** positive integers n,

$$x^n + y^n = (x+y)\left(x^{n-1} - x^{n-2}y + x^{n-3}y^2 + \cdots + y^{n-1}\right).$$

Important Lemma

Example. Prove that if $a \equiv b \pmod{n}$, then $a^n \equiv b^n \pmod{n^2}$.

Solution. We use our difference of nth powers factorization:

$$a^n - b^n = (a-b)\left(a^{n-1} + a^{n-2}b + \cdots + b^{n-1}\right).$$

Since $a \equiv b \pmod{n}$, the first term in the product is divisible by n. Furthermore, substituting the congruence into the second term gives

$$a^{n-1} + a^{n-2}b + \cdots + b^{n-1} \equiv \underbrace{b^{n-1} + b^{n-1} + \cdots + b^{n-1}}_{\text{n terms}} \equiv 0 \pmod{n}.$$

Therefore, the product is divisible by n^2.

Divisor Problem

Example. Find a divisor between 2000 and 3000 of $85^9 - 21^9 + 6^9$.

Solution. Let $N = 85^9 - 21^9 + 6^9$. Note 6^9 is divisible by 64 and

$$85 \equiv 21 \pmod{64} \implies 85^9 \equiv 21^9 \pmod{64}.$$

Therefore, N is divisible by 64. Since $21 \equiv 6 \pmod{5}$,

$$N \equiv 0 - 6^9 + 6^9 \equiv 0 \pmod{5}.$$

Finally, since $85 \equiv 1 \pmod{7}$ and $6 \equiv -1 \pmod{7}$, we see that

$$N \equiv 1^9 - 0 + (-1)^9 \equiv 0 \pmod{7}.$$

Therefore, the desired divisor between 2000 and 3000 is $2^6 \cdot 5^1 \cdot 7^1 = \mathbf{2240}$.

Fun Challenge Problems

Example 1. (Mandelbrot) Determine the positive integer a such that $x^8 + 5x^6 + 13x^4 + 20x^2 + 36$ is evenly divisible by $x^2 - x + a$.

Example 2. (AIME) Find integer values a and b such that $x^2 - x - 1$ is a factor of $ax^{17} + bx^{16} + 1$. *Hint:* Use Binet's Formula.

Example 3. Prove that the harmonic sum

$$H_n = \frac{1}{1} + \frac{1}{2} + \cdots + \frac{1}{n} = \sum_{k=1}^{n} \frac{1}{k}$$

is never an integer for $n \geq 2$. *Hint:* Consider the 2-adic valuation.

Example 4. (Cassini's Identity) Prove that $F_{n+1}F_{n-1} - F_n^2 = (-1)^2$.

Example 5. Prove that 60 divides xyz for a Pythagorean triple (x, y, z).

Example 6. Prove that the radius of the inscribed circle of a Pythagorean triple is always an integer. *Hint:* The area of a triangle is $r/2(x + y + z)$.