Primes and Polynomials

Lecture 4

Justin Stevens

Outline

Primes and Composites

Definition. A **prime number** p is a natural number whose only positive divisors are 1 and p. The first several are $2, 3, 5, 7, 11, 13, 17, 23, 29, 31, \cdots$.

Definition. A **composite number** c is a natural number that has divisors other than 1 and c. The first several are $4, 6, 8, 9, 10, 12, 14, 15, 16, \cdots$.

Amogst the composites, $4 = 2 \cdot 2$, $6 = 2 \cdot 3$, $8 = 2 \cdot 4$, $9 = 3 \cdot 3$, $10 = 2 \cdot 5$. Notice all composites can be written in the form $c = ab$ where $a, b > 1$.

Example 1. Determine if 211, 1001, or 9409 are prime.

Primality

Example. Determine if 211, 1001, or 9409 are prime.

Prime Puzzles

Example 2. Find all positive integers n such that $n^4 + 4$ is prime.

Example 3. Prove that if a and n are positive integers with $n > 1$ such that $a^n - 1$ is prime, then $a = 2$ and n is prime.

Example 4. Show that for any positive integer n, we can find n consecutive composite numbers.

$n^4 + 4$ prime

Example. Find all positive integers n such that $n^4 + 4$ is prime.

In order to factorize this, we add $4n^2$ to make this a perfect square:

$$n^4 + 4n^2 + 4 = \left(n^2 + 2\right)^2.$$

Therefore, using difference of squares,

$$\begin{aligned} n^4 + 4 &= \left(n^2 + 2\right)^2 - (2n)^2 \\ &= \left(n^2 - 2n + 2\right)\left(n^2 + 2n + 2\right) \\ &= \left((n-1)^2 + 1\right)\left((n+1)^2 + 1\right). \end{aligned}$$

In order for this expression to be prime, one of the factors must be 1. This is only true when $n = 1$ giving the prime 5.

Sophie Germain Identity

Theorem. $a^2 + 4b^2 = \left(a^2 + 2b^2 + 2ab\right)\left(a^2 + 2b^2 - 2ab\right).$

Mersenne Primes

Example. Prove that if a and n are positive integers with $n > 1$ such that $a^n - 1$ is prime, then $a = 2$ and n is prime.

From $a^n - 1 = (a-1)\left(a^{n-1} + a^{n-2} + \cdots + 1\right)$, we have $a = 2$.

Mersenne Primes

Example. Prove that if a and n are positive integers with $n > 1$ such that $a^n - 1$ is prime, then $a = 2$ and n is prime.

From $a^n - 1 = (a-1)\left(a^{n-1} + a^{n-2} + \cdots + 1\right)$, we have $a = 2$.

We now show that n is prime. Assume for the sake of contradiction that n is composite, implying $n = ab$. Then

$$\begin{aligned} 2^{ab} - 1 &= (2^a - 1)\left(1 + 2^a + 2^{2a} + \cdots + 2^{a\cdot(b-1)}\right) \\ &= \left(2^b - 1\right)\left(1 + 2^b + 2^{2b} + \cdots + 2^{b\cdot(a-1)}\right). \end{aligned}$$

Hence, n must be prime.

Mersenne Primes

Example. Prove that if a and n are positive integers with $n > 1$ such that $a^n - 1$ is prime, then $a = 2$ and n is prime.

From $a^n - 1 = (a-1)\left(a^{n-1} + a^{n-2} + \cdots + 1\right)$, we have $a = 2$.

We now show that n is prime. Assume for the sake of contradiction that n is composite, implying $n = ab$. Then

$$\begin{aligned} 2^{ab} - 1 &= (2^a - 1)\left(1 + 2^a + 2^{2a} + \cdots + 2^{a\cdot(b-1)}\right) \\ &= \left(2^b - 1\right)\left(1 + 2^b + 2^{2b} + \cdots + 2^{b\cdot(a-1)}\right). \end{aligned}$$

Hence, n must be prime.

Definition. Numbers of the form $2^p - 1$ are known as **Mersenne primes**. The largest known prime number is $2^{74,207,281} - 1$, a number with over 22 million digits! It was found by the Great Internet Mersenne Prime Search.

Consecutive prime numbers

Example. Show that for any positive integer n, we can find n consecutive composite numbers.

Since factorials have a lot of prime factors, we think to use them. For instance, consider $6! = 2 \cdot 3 \cdot 4 \cdot 5 \cdot 6$. Note that if we add $2, 3, 4, 5$ or 6 to $6!$ the resulting value will be composite:

$$6! + 2 = 2\,(1 + 360) = 722$$
$$6! + 3 = 3\,(1 + 240) = 723$$
$$6! + 4 = 4\,(1 + 180) = 724$$
$$6! + 5 = 5\,(1 + 144) = 725$$
$$6! + 6 = 6\,(1 + 120) = 726.$$

In general, if we consider the set

$$\{(n+1)! + 2, (n+1)! + 3, (n+1)! + 4, \cdots, (n+1)! + n + 1\},$$

we will have n consecutive composite numbers.

Fundamental Theorem of Arithmetic

In 1801, Gauss proved the Fundamental Theorem of Arithmetic in his book "Disquisitiones Arithmeticae".

Theorem. Every integer at least 2 is either prime itself or is the unique product of primes.

This theorem is the reason 1 is not a prime number; otherwise, the product would not be unique! Before proving the Fundamental Theorem of Arithmetic, we revisit our friend Euclid and learn about induction.

Euclid's Lemma

"If two numbers by multiplying one another make some number, and any prime number measure the product, it will also measure one of the original numbers."
- Euclid's Elements, Book VII, Proposition 30"

In other words, if prime $p \mid ab$ for integers a, b, then $p \mid a$ or $p \mid b$.

⋆ Induction

Another key factor in the proof of the Fundamental Theorem of Arithmetic is the method of **mathematical induction**.

Definition. In order to prove a statement $P(x)$ is true for all positive integers $x \geq a$, it suffices to show this in two parts:

- *The base case:* $P(a)$ is true.
- *The inductive step:* For all positive integers $k \geq a$, $P(k)$ being true implies $P(k+1)$ is also true.

This is a domino effect where one domino knocks down the next.

⋆ Example of Induction

For instance, suppose I wish to show the identity

$$1 + 2 + 3 + \cdots + n = \frac{n(n+1)}{2}$$

holds for all $n \geq 1$. I begin by showing the identity holds for $n = 1$: $1 = \frac{1 \cdot 2}{2}$. I then show that if the identity is true for $n = k$, then it is also true for $n = k + 1$. The inductive *hypothesis* is that $1 + 2 + 3 + \cdots + k = \frac{k(k+1)}{2}$. We use this to show the identity holds for $n = k + 1$. Indeed, note that

$$\begin{aligned}(1 + 2 + 3 + \cdots + k) + k + 1 &= \frac{k(k+1)}{2} + k + 1 \\ &= (k+1)\left(\frac{k}{2} + 1\right) \\ &= \frac{(k+1)(k+2)}{2}.\end{aligned}$$

⋆ Strong Induction

Definition. Replace the inductive step with: If $P(a), P(a+1), P(a+2), P(a+3), \cdots, P(k-1), P(k)$ being true *implies* that $P(k+1)$ is also true. The way I visualize strong induction is below:

$$\begin{aligned} P(a) &\implies P(a+1) \\ P(a), P(a+1) &\implies P(a+2) \\ P(a), P(a+1), P(a+2) &\implies P(a+3) \\ &\cdots \end{aligned}$$

It is a slightly more confusing domino effect! Knowing strong induction will be particularly useful when you take an analysis class down the road.

⋆ Proof of Fundamental Theorem of Arithmetic I

While the notation may be confusing now, after we see strong induction in action, it will make more sense!

Theorem. Every integer at least 2 is either prime itself or is the unique product of primes.

Proof. We prove the Fundamental Theorem of Arithmetic. There are two parts for the proof: showing the existence of a prime factorization, and the uniqueness of the prime factorization. We begin with the existence part.

We use the method of strong induction. We desire to show that all positive integers greater than or equal to 2 are either prime or can be expressed as the product of primes. To begin with, as a base case, 2 itself is prime.

⋆ Existence Proof

Theorem. Every integer at least 2 is either prime itself or is the unique product of primes.

Furthermore, using the strong induction hypothesis, assume that we have proven the the existence of a prime factorization for all integers y with $2 \leq y \leq k$. We then prove the existence for $k + 1$. We have two cases:

⋆ Existence Proof

Theorem. Every integer at least 2 is either prime itself or is the unique product of primes.

Furthermore, using the strong induction hypothesis, assume that we have proven the the existence of a prime factorization for all integers y with $2 \leq y \leq k$. We then prove the existence for $k + 1$. We have two cases:

- If $k + 1$ itself is prime, then this satisfies the first condition of the Fundamental Theorem of Arithmetic.

⋆ Existence Proof

Theorem. Every integer at least 2 is either prime itself or is the unique product of primes.

Furthermore, using the strong induction hypothesis, assume that we have proven the the existence of a prime factorization for all integers y with $2 \leq y \leq k$. We then prove the existence for $k+1$. We have two cases:

- If $k+1$ itself is prime, then this satisfies the first condition of the Fundamental Theorem of Arithmetic.
- If $k+1$ is composite, it is the product of two numbers a, b greater than 1. By the strong induction hypothesis, since $2 \leq a, b < k+1$, both a and b are the product of primes. Therefore, $k+1 = ab$ is also the product of primes.

⋆ Existence Proof

Theorem. Every integer at least 2 is either prime itself or is the unique product of primes.

Furthermore, using the strong induction hypothesis, assume that we have proven the the existence of a prime factorization for all integers y with $2 \leq y \leq k$. We then prove the existence for $k+1$. We have two cases:

- If $k+1$ itself is prime, then this satisfies the first condition of the Fundamental Theorem of Arithmetic.
- If $k+1$ is composite, it is the product of two numbers a, b greater than 1. By the strong induction hypothesis, since $2 \leq a, b < k+1$, both a and b are the product of primes. Therefore, $k+1 = ab$ is also the product of primes.

Since in both cases, $k+1$ has a prime factorization, by the method of strong induction, we have proved the existence of a prime factorization.

⋆ Uniqueness Proof

For the uniqueness part, we use proof by contradiction. Consider the set S of positive integers that do not have a unique prime factorization. Assume for the sake of contradiction that S is non-empty.

⋆ Uniqueness Proof

For the uniqueness part, we use proof by contradiction. Consider the set S of positive integers that do not have a unique prime factorization. Assume for the sake of contradiction that S is non-empty.

Then, using the well-ordering principle, S must have a least element, say n. Let the two possible prime factorizations of n be

$$n = p_1 p_2 p_3 \cdots p_s = q_1 q_2 q_3 \cdots q_r.$$

I will show that there is a smaller value in S than n.

⋆ Uniqueness Proof

For the uniqueness part, we use proof by contradiction. Consider the set S of positive integers that do not have a unique prime factorization. Assume for the sake of contradiction that S is non-empty.

Then, using the well-ordering principle, S must have a least element, say n. Let the two possible prime factorizations of n be

$$n = p_1 p_2 p_3 \cdots p_s = q_1 q_2 q_3 \cdots q_r.$$

I will show that there is a smaller value in S than n.

We see that $p_1 \mid q_1 q_2 q_3 \cdots q_r$. By Euclid's Lemma, we must have $p_1 \mid q_j$ for some $1 \leq j \leq r$. However, since they are primes, this implies that $p_1 = q_j$. We cancel out this similar term to get

$$\frac{n}{p_1} = \frac{n}{q_j} = p_2 p_3 \cdots p_s = q_1 q_2 q_3 \cdots q_{j-1} q_{j+1} \cdots q_r.$$

⋆ Uniqueness Proof

For the uniqueness part, we use proof by contradiction. Consider the set S of positive integers that do not have a unique prime factorization. Assume for the sake of contradiction that S is non-empty.

Then, using the well-ordering principle, S must have a least element, say n. Let the two possible prime factorizations of n be

$$n = p_1 p_2 p_3 \cdots p_s = q_1 q_2 q_3 \cdots q_r.$$

I will show that there is a smaller value in S than n.

We see that $p_1 \mid q_1 q_2 q_3 \cdots q_r$. By Euclid's Lemma, we must have $p_1 \mid q_j$ for some $1 \leq j \leq r$. However, since they are primes, this implies that $p_1 = q_j$. We cancel out this similar term to get

$$\frac{n}{p_1} = \frac{n}{q_j} = p_2 p_3 \cdots p_s = q_1 q_2 q_3 \cdots q_{j-1} q_{j+1} \cdots q_r.$$

We have shown that $\frac{n}{p_1} = \frac{n}{q_j}$ does not have a unique prime factorization! This contradicts the minimality of n, and prime factorization is unique.

Infitude of Primes

Example 5. Show that there are an infinite number of primes.

Assume for the sake of contradiction that there are a finite number of primes, namely $\{p_1, p_2, p_3, \cdots, p_k\}$. Consider the number

$$N = p_1 p_2 p_3 \cdots p_k + 1.$$

Infitude of Primes

Example 6. Show that there are an infinite number of primes.

Assume for the sake of contradiction that there are a finite number of primes, namely $\{p_1, p_2, p_3, \cdots, p_k\}$. Consider the number

$$N = p_1 p_2 p_3 \cdots p_k + 1.$$

Observe that for $1 \leq i \leq k$, we have $p_i \nmid N$. However, we assumed that this set consisted of all the primes. Therefore, N must either have a prime divisor from outside this set, or N itself must be prime. Either way, we have constructed a new prime number, contradiction.

Infitude of Primes

Example 7. Show that there are an infinite number of primes.

Assume for the sake of contradiction that there are a finite number of primes, namely $\{p_1, p_2, p_3, \cdots, p_k\}$. Consider the number

$$N = p_1 p_2 p_3 \cdots p_k + 1.$$

Observe that for $1 \leq i \leq k$, we have $p_i \nmid N$. However, we assumed that this set consisted of all the primes. Therefore, N must either have a prime divisor from outside this set, or N itself must be prime. Either way, we have constructed a new prime number, contradiction.

Warning: It is a common misconception that this proof implies N must always be prime. However, we see that

$$2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 13 + 1 = 30031 = 59 \cdot 509$$

is not a prime number.

Canonical Prime Factorization

The preferred method for writing the prime factorization of a positive integer n is

$$n = \prod_{j=1}^{k} \left(p_j^{e_j} \right) = p_1^{e_1} p_2^{e_2} \cdots p_k^{e_k}.$$

The $\prod$ symbol is similar to the $\sum$ symbol, except we multiply all the terms! Writing prime factorizations in this form makes it easier to compute the gcd and lcm of two numbers. It also allows us to do many problems involving divisors!

Canonical Prime Factorization Puzzles

Example 8. Note that $6! = 720$ ends in one zero. The number

$$25! = 15511210043330985984000000$$

ends in 6 zeros. How many zeros does 100! end in?

Example 9. Find the number of ordered triples (x, y, z) for which $xyz = 2400$ over the positive integers.

How Does Zero Work?

Example. How many zeros does 100! end in?

Zeros at the end of a number come from powers of 10. For instance,

$$25! = 15511210043330985984 \times 10^6.$$

The problem is the same as finding the largest power of 10 that divides 100!.

Definition. Define $v_p(n)$ to be the integer e such that $p^e \mid n$, but $p^{e+1} \nmid n$. Another way to write this is $p^e \parallel n$.

See $v_2(48) = 4$ and $v_5(200) = 2$ since $48 = 2^4 \cdot 3^1$ and $200 = 5^2 \cdot 2^3$.

We desire to find $v_{10}(100!)$. Since $10 = 2 \cdot 5$, the largest power of 10 that divides 100! is the **minimum** of $v_2(100!)$ and $v_5(100!)$.

V for Vendetta

Example. How many zeros does 100! end in?

We begin by calculating $v_2(100!)$. We write out

$$100! = 100 \cdot 99 \cdot 98 \cdot 97 \cdots 3 \cdot 2 \cdot 1.$$

Consider all the numbers in the product above. How many of them are multiples of 2? Multiples of 4? Multiples of 8?

V for Vendetta

Example. How many zeros does 100! end in?

We begin by calculating $v_2(100!)$. We write out

$$100! = 100 \cdot 99 \cdot 98 \cdot 97 \cdots 3 \cdot 2 \cdot 1.$$

Consider all the numbers in the product above. How many of them are multiples of 2? Multiples of 4? Multiples of 8?

The number of multiples of 2 is the number of even numbers in the product. Half of the numbers are even, hence there are $\frac{100}{2} = 50$ multiples of 2.

For other powers of 2, we must introduce the floor function.

V for Vendetta

Example. How many zeros does 100! end in?

We begin by calculating $v_2(100!)$. We write out

$$100! = 100 \cdot 99 \cdot 98 \cdot 97 \cdots 3 \cdot 2 \cdot 1.$$

Consider all the numbers in the product above. How many of them are multiples of 2? Multiples of 4? Multiples of 8?

The number of multiples of 2 is the number of even numbers in the product. Half of the numbers are even, hence there are $\frac{100}{2} = 50$ multiples of 2.

For other powers of 2, we must introduce the floor function.

Definition. The floor function of a real number x is defined as the largest integer less than or equal to x. In other words, it is the result of truncating x. For instance, $\lfloor 3.14159 \rfloor = 3$ and $\lfloor -16.3 \rfloor = -17$.

Computing $v_2(100!)$

Example. Compute $v_2(100!)$.

Using the floor function, we can find that

- There are $\lfloor \frac{100}{2} \rfloor = 50$ multiples of 2.
- There are $\lfloor \frac{100}{4} \rfloor = 25$ multiples of 4.
- There are $\lfloor \frac{100}{8} \rfloor = 12$ multiples of 8.
- There are $\lfloor \frac{100}{16} \rfloor = 6$ multiples of 16.
- There are $\lfloor \frac{100}{32} \rfloor = 3$ multiples of 32.
- There are $\lfloor \frac{100}{64} \rfloor = 1$ multiple of 64.

I claim that the number of powers of 2 in 100! is the sum of all the numbers above: $50 + 25 + 12 + 6 + 3 + 1 = 97$.

Computing $v_2(12!)$

Consider the following table:

	1	2	3	4	5	6	7	8	9	10	11	12
2^1		✓		✓		✓		✓		✓		✓
2^2				✓				✓				✓
2^3								✓				

Computing $v_2(12!)$

Consider the following table:

	1	2	3	4	5	6	7	8	9	10	11	12
2^1		✓		✓		✓		✓		✓		✓
2^2				✓				✓				✓
2^3								✓				

The number of checkmarks is equal to $v_2(12!)$. Adding them row-wise, we see that

$$v_2(12!) = \lfloor \frac{12}{2} \rfloor + \lfloor \frac{12}{4} \rfloor + \lfloor \frac{12}{8} \rfloor = 6 + 3 + 1 = 10.$$

Computing $v_2(12!)$

Consider the following table:

	1	2	3	4	5	6	7	8	9	10	11	12
2^1		✓		✓		✓		✓		✓		✓
2^2				✓				✓				✓
2^3								✓				

The number of checkmarks is equal to $v_2(12!)$. Adding them row-wise, we see that

$$v_2(12!) = \lfloor \frac{12}{2} \rfloor + \lfloor \frac{12}{4} \rfloor + \lfloor \frac{12}{8} \rfloor = 6 + 3 + 1 = 10.$$

The same logic applies to $v_2(100!) = 97$. Are we finished with the problem yet?

Finishing the Problem

Example. How many zeros does 100! end in?

Earlier we determined $v_{10}(100!) = \min\left(v_2(100!), v_5(100!)\right)$.

Finishing the Problem

Example. How many zeros does 100! end in?

Earlier we determined $v_{10}(100!) = \min\left(v_2(100!), v_5(100!)\right)$.

We see that

$$v_5(100!) = \lfloor \frac{100}{5} \rfloor + \lfloor \frac{100}{25} \rfloor = 20 + 4 = 24.$$

Hence, there are $\boxed{24}$ zero's at the end of 100!.

Finishing the Problem

Example. How many zeros does 100! end in?

Earlier we determined $v_{10}(100!) = \min\left(v_2(100!), v_5(100!)\right)$.

We see that

$$v_5(100!) = \lfloor \frac{100}{5} \rfloor + \lfloor \frac{100}{25} \rfloor = 20 + 4 = 24.$$

Hence, there are $\boxed{24}$ zero's at the end of 100!.

Using Wolfram-Alpha, we can verify that 100! = 106992388562667004907159682643816214685929638952175999932299156089414639761565182862536979208272237582511852109168640000000000000000000000.

Legendre's Formula

Adrien-Marie Legendre (1752-1833) generalized this problem.

Theorem. The number of powers of a prime p that divide into $n!$ is

$$v_p(n!) = \sum_{k=1}^{\infty} \left(\left\lfloor \frac{n}{p^k} \right\rfloor \right).$$

$xyz = 2400$ over $\mathbb{Z}$

Example. Find the number of ordered triples (x, y, z) for which $xyz = 2400$ over the positive integers.

We begin by prime factorizing $2400 = 2^5 \cdot 3^1 \cdot 5^2$. We write

$$x = 2^{x_2}3^{x_3}5^{x_5};\ y = 2^{y_2}3^{y_3}5^{y_5};\ z = 2^{z_2}3^{z_3}5^{z_5}.$$

Since $xyz = 2400$, this is equivalent to having

$$\begin{aligned} x_2 + y_2 + z_2 &= 5 \\ x_3 + y_3 + z_3 &= 1 \\ x_5 + y_5 + z_5 &= 2. \end{aligned}$$

How many integer triplets can you find for (x_3, y_3, z_3) and (x_5, y_5, z_5)?

$xyz = 2400$ over $\mathbb{Z}$

Example. Find the numbered of integer triplets satisfying

$$x_3 + y_3 + z_3 = 1$$
$$x_5 + y_5 + z_5 = 2.$$

Since $x_3 + y_3 + z_3 = 1$, we have **3** possible triplets for (x_3, y_3, z_3), namely

$$(x_3, y_3, z_3) = (1, 0, 0), (0, 1, 0), (0, 0, 1).$$

$xyz = 2400$ over $\mathbb{Z}$

Example. Find the numbered of integer triplets satisfying

$$x_3 + y_3 + z_3 = 1$$
$$x_5 + y_5 + z_5 = 2.$$

Since $x_3 + y_3 + z_3 = 1$, we have **3** possible triplets for (x_3, y_3, z_3), namely

$$(x_3, y_3, z_3) = (1, 0, 0), (0, 1, 0), (0, 0, 1).$$

Since $x_5 + y_5 + z_5 = 2$, we have **6** possible triplets for (x_5, y_5, z_5), namely

$$(x_5, y_5, z_5) = (2, 0, 0), (0, 2, 0), (0, 0, 2), (1, 1, 0), (1, 0, 1), (0, 1, 1).$$

How many integers triplets are there for $x_2 + y_2 + z_2 = 5$?

$xyz = 2400$ over $\mathbb{Z}$

Example. Find the number of triplets such that $x_2 + y_2 + z_2 = 5$.

We could begin listing possible triplets, but there are far too many to list.

We try to think of a clever method. We use a method in combinatorics known as **stars and bars** by creating a bijection between the number of ordered triplets (x_2, y_2, z_2) and the rearrangement of stars and bars.

$xyz = 2400$ over $\mathbb{Z}$

Example. Find the number of triplets such that $x_2 + y_2 + z_2 = 5$.

We could begin listing possible triplets, but there are far too many to list.

We try to think of a clever method. We use a method in combinatorics known as **stars and bars** by creating a bijection between the number of ordered triplets (x_2, y_2, z_2) and the rearrangement of stars and bars.

We desire to distribute five $1's$ to three variables. Therefore, we write out the five $1's$ as such: 1 1 1 1 1. We desire to divide this into three groups, therefore, we place two dividers, which we symbolize by blue x's:

$$1\, x\, 1\ 1\, x\, 1\ 1$$

In the above configuration, we have $(x_2, y_2, z_2) = (1, 2, 2)$.

$xyz = 2400$ over $\mathbb{Z}$

Example. Find the number of triplets such that $x_2 + y_2 + z_2 = 5$.

We could begin listing possible triplets, but there are far too many to list.

We try to think of a clever method. We use a method in combinatorics known as **stars and bars** by creating a bijection between the number of ordered triplets (x_2, y_2, z_2) and the rearrangement of stars and bars.

We desire to distribute five $1's$ to three variables. Therefore, we write out the five $1's$ as such: 1 1 1 1 1. We desire to divide this into three groups, therefore, we place two dividers, which we symbolize by blue x's:

$$1\,x\,1\;\;1\,x\,1\;\;1$$

In the above configuration, we have $(x_2, y_2, z_2) = (1, 2, 2)$.

The number of rearrangements of the objects above is $\binom{7}{2} = \frac{7 \cdot 6}{2} = \mathbf{21}$.

$xyz = 2400$ over $\mathbb{Z}$

Example. Find the number of ordered triples (x, y, z) for which $xyz = 2400$ over the positive integers.

We begin by prime factorizing $2400 = 2^5 \cdot 3^1 \cdot 5^2$. We write

$$x = 2^{x_2}3^{x_3}5^{x_5};\ y = 2^{y_2}3^{y_3}5^{y_5};\ z = 2^{z_2}3^{z_3}5^{z_5}.$$

Since $xyz = 2400$, this is equivalent to having

$$\begin{aligned} x_2 + y_2 + z_2 &= 5 \\ x_3 + y_3 + z_3 &= 1 \\ x_5 + y_5 + z_5 &= 2. \end{aligned}$$

$xyz = 2400$ over $\mathbb{Z}$

Example. Find the number of ordered triples (x, y, z) for which $xyz = 2400$ over the positive integers.

We begin by prime factorizing $2400 = 2^5 \cdot 3^1 \cdot 5^2$. We write

$$x = 2^{x_2} 3^{x_3} 5^{x_5};\ y = 2^{y_2} 3^{y_3} 5^{y_5};\ z = 2^{z_2} 3^{z_3} 5^{z_5}.$$

Since $xyz = 2400$, this is equivalent to having

$$\begin{aligned} x_2 + y_2 + z_2 &= 5 \\ x_3 + y_3 + z_3 &= 1 \\ x_5 + y_5 + z_5 &= 2. \end{aligned}$$

We found there are **21** triplets for (x_2, y_2, z_2), **3** triplets for (x_3, y_3, z_3), and **6** triplets for (x_5, y_5, z_5). Therefore, the answer is $21 \cdot 3 \cdot 6 = \boxed{378}$.

Greatest Common Divisor and Least Common Multiple

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

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

Then,

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

Note that $\gcd(a,b)\operatorname{lcm}[a,b] = 2^{6+9} \cdot 3^{1+5} \cdot 7^2 = ab$. This is true in general because $\min(a_j,b_j) + \max(a_j,b_j) = a_j + b_j$.

Least Common Multiples

Example 10. For how many values of k is 12^{12} the least common multiple of 6^6, 8^8, and k? *

Example 11. Let $[r, s]$ denote the least common multiple of positive integers r and s. Find the number of ordered triples a, b, c such that $[a, b] = 1000, [b, c] = 2000, [c, a] = 2000$. †

* Source: 1998 AIME

† Source: 1987 AIME

1998 AIME

Example. For how many values of k is 12^{12} the least common multiple of 6^6, 8^8, and k? ‡

We find the prime factorizations of these numbers. We have

$$12^{12} = 2^{24} \cdot 3^{12}, 6^6 = 2^6 \cdot 3^6 \text{ and } 8^8 = 2^{24}.$$

Let $k = 2^{k_1}3^{k_2}$. We then rewrite the equation as

$$\text{lcm}[2^6 \cdot 3^6, 2^{24}, 2^{k_1}3^{k_2}] = 2^{24} \cdot 3^{12}.$$

Since none of the first two terms have a factor of 3^{12}, we must have $k_2 = 12$.
On the other hand, the second term has a factor of 2^{24}. Therefore, we must have $0 \leq k_1 \leq 24$, giving $\boxed{25}$ possible values of k.

‡ Source: 1998 AIME

1987 AIME

Example. Let $[r, s]$ denote the least common multiple of positive integers r and s. Find the number of ordered triples a, b, c such that $[a, b] = 1000, [b, c] = 2000, [c, a] = 2000$.

Notice that $1000 = 2^3 \times 5^3, 2000 = 2^4 \times 5^3$. Since we are working with least common multiples, set $a = 2^{a_1}5^{a_2}, b = 2^{b_1}5^{b_2}, c = 2^{c_1}5^{c_2}$.

1987 AIME

Example. Let $[r, s]$ denote the least common multiple of positive integers r and s. Find the number of ordered triples a, b, c such that $[a, b] = 1000, [b, c] = 2000, [c, a] = 2000$.

Notice that $1000 = 2^3 \times 5^3, 2000 = 2^4 \times 5^3$. Since we are working with least common multiples, set $a = 2^{a_1}5^{a_2}, b = 2^{b_1}5^{b_2}, c = 2^{c_1}5^{c_2}$.

We see that $v_2([a, b]) = 3$ and $v_2([b, c]) = v_2([c, a]) = 4$. Therefore, we must have $c_1 = 4$ and at least one of a_1, b_1 equals 3. Hence, we have $(a_1, b_1) = (0, 3), (1, 3), (2, 3), (3, 3), (3, 2), (3, 1), (3, 0)$, for a total of **7**.

1987 AIME

Example. Let $[r, s]$ denote the least common multiple of positive integers r and s. Find the number of ordered triples a, b, c such that $[a, b] = 1000, [b, c] = 2000, [c, a] = 2000$.

Notice that $1000 = 2^3 \times 5^3, 2000 = 2^4 \times 5^3$. Since we are working with least common multiples, set $a = 2^{a_1}5^{a_2}, b = 2^{b_1}5^{b_2}, c = 2^{c_1}5^{c_2}$.

We see that $v_2([a, b]) = 3$ and $v_2([b, c]) = v_2([c, a]) = 4$. Therefore, we must have $c_1 = 4$ and at least one of a_1, b_1 equals 3. Hence, we have $(a_1, b_1) = (0, 3), (1, 3), (2, 3), (3, 3), (3, 2), (3, 1), (3, 0)$, for a total of $\mathbf{7}$.

Now, we consider the powers of 5. We note that $v_5([a, b]) = 3, v_5([a, c]) = 3, v_5([b, c]) = 3$. This gives us four cases:

$$(a_2, b_2, c_2) = (3, 3, 3), (3, 3, x), (3, x, 3), (x, 3, 3).$$

We know that $0 \leq x \leq 2$, therefore, there are 3 possibilities for the x's. Hence, there are a total of $3 \cdot 3 + 1 = \mathbf{10}$ possibilities for the power of 5.

1987 AIME

Example. Let $[r, s]$ denote the least common multiple of positive integers r and s. Find the number of ordered triples a, b, c such that $[a, b] = 1000, [b, c] = 2000, [c, a] = 2000$.

Notice that $1000 = 2^3 \times 5^3, 2000 = 2^4 \times 5^3$. Since we are working with least common multiples, set $a = 2^{a_1}5^{a_2}, b = 2^{b_1}5^{b_2}, c = 2^{c_1}5^{c_2}$.

We see that $v_2([a, b]) = 3$ and $v_2([b, c]) = v_2([c, a]) = 4$. Therefore, we must have $c_1 = 4$ and at least one of a_1, b_1 equals 3. Hence, we have $(a_1, b_1) = (0, 3), (1, 3), (2, 3), (3, 3), (3, 2), (3, 1), (3, 0)$, for a total of $\mathbf{7}$.

Now, we consider the powers of 5. We note that $v_5([a, b]) = 3, v_5([a, c]) = 3, v_5([b, c]) = 3$. This gives us four cases:

$$(a_2, b_2, c_2) = (3, 3, 3), (3, 3, x), (3, x, 3), (x, 3, 3).$$

We know that $0 \leq x \leq 2$, therefore, there are 3 possibilities for the x's. Hence, there are a total of $3 \cdot 3 + 1 = \mathbf{10}$ possibilities for the power of 5.

In conclusion, there is a total of $7 \cdot 10 = \boxed{70}$ ordered triples a, b, c which

Outline

Polynomial Division

The division algorithm also works in $\mathbb{Q}[x]$, the set of polynomials with rational coefficients, and $\mathbb{R}[x]$, the set of all polynomials with real coefficients. For the sake of our study, we will only focus on $\mathbb{Q}[x]$.

Theorem. If $n(x)$ and $d(x)$ are two polynomials, then we can find a unique quotient and remainder polynomial, $q(x), r(x) \in \mathbb{Q}[x]$, such that

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

Example 12. Calculate $q(x)$ and $r(x)$ for $n(x) = x^4 + 3x^3 + 10$ and $d(x) = x^2 - x$.

Division Example I

Example. Calculate $q(x)$ and $r(x)$ for $n(x) = x^4 + 3x^3 + 10$ and $d(x) = x^2 - x$.

We divide the leading term of $n(x)$ by the leading term of $d(x)$: $\frac{x^4}{x^2} = x^2$.

Division Example I

Example. Calculate $q(x)$ and $r(x)$ for $n(x) = x^4 + 3x^3 + 10$ and $d(x) = x^2 - x$.

We divide the leading term of $n(x)$ by the leading term of $d(x)$: $\frac{x^4}{x^2} = x^2$.
We now multiply $d(x)$ by x^2 and subtract the result from $n(x)$:

$$x^4 + 3x^3 + 10 = (x^2 - x)(x^2) + (4x^3 + 10).$$

Division Example I

Example. Calculate $q(x)$ and $r(x)$ for $n(x) = x^4 + 3x^3 + 10$ and $d(x) = x^2 - x$.

We divide the leading term of $n(x)$ by the leading term of $d(x)$: $\frac{x^4}{x^2} = x^2$. We now multiply $d(x)$ by x^2 and subtract the result from $n(x)$:

$$x^4 + 3x^3 + 10 = (x^2 - x)(x^2) + (4x^3 + 10).$$

To eliminate the cubic term, we divide the leading term of $q(x)$, $4x^3$ by x^2: $\frac{4x^3}{x^2} = 4x$. We add this to the quotient:

$$x^4 + 3x^3 + 10 = (x^2 - x)(x^2 + 4x) + (4x^2 + 10.)$$

Division Example I

Example. Calculate $q(x)$ and $r(x)$ for $n(x) = x^4 + 3x^3 + 10$ and $d(x) = x^2 - x$.

We divide the leading term of $n(x)$ by the leading term of $d(x)$: $\frac{x^4}{x^2} = x^2$. We now multiply $d(x)$ by x^2 and subtract the result from $n(x)$:

$$x^4 + 3x^3 + 10 = (x^2 - x)(x^2) + (4x^3 + 10).$$

To eliminate the cubic term, we divide the leading term of $q(x)$, $4x^3$ by x^2: $\frac{4x^3}{x^2} = 4x$. We add this to the quotient:

$$x^4 + 3x^3 + 10 = (x^2 - x)(x^2 + 4x) + (4x^2 + 10.)$$

Can we stop here? No, since $\deg(r(x)) = 2 = \deg(d(x))$.

Division Example II

Example. Calculate $q(x)$ and $r(x)$ for $n(x) = x^4 + 3x^3 + 10$ and $d(x) = x^2 - x$.

Therefore, in order to remove the quadratic term from the remainder, we divide this term, $4x^2$, by the leading term of $d(x)$, x^2: $\frac{4x^2}{x^2} = 4$. We then add this to the quotient, and subtract, in order to get

Division Example II

Example. Calculate $q(x)$ and $r(x)$ for $n(x) = x^4 + 3x^3 + 10$ and $d(x) = x^2 - x$.

Therefore, in order to remove the quadratic term from the remainder, we divide this term, $4x^2$, by the leading term of $d(x)$, x^2: $\frac{4x^2}{x^2} = 4$. We then add this to the quotient, and subtract, in order to get

$$x^4 + 3x^3 + 10 = (x^2 - x)(x^2 + 4x + 4) + (4x + 10).$$

Division Example II

Example. Calculate $q(x)$ and $r(x)$ for $n(x) = x^4 + 3x^3 + 10$ and $d(x) = x^2 - x$.

Therefore, in order to remove the quadratic term from the remainder, we divide this term, $4x^2$, by the leading term of $d(x)$, x^2: $\frac{4x^2}{x^2} = 4$. We then add this to the quotient, and subtract, in order to get

$$x^4 + 3x^3 + 10 = (x^2 - x)(x^2 + 4x + 4) + (4x + 10).$$

Since the degree of the remainder is less than the degree of $d(x)$, we are finished. Therefore, $q(x) = \boxed{x^2 + 4x + 4}$ and $r(x) = \boxed{4x + 10}$.

Division Challenges

Example 13. What is the largest positive integer n such that $n^3 + 100$ is divisible by $n + 10$? [§]

[§] Source: 1986 AIME

1986 AIME Problem

Example. Find the largest integer n such that n^3+100 is divisible by $n+10$.

We begin by dividing $n^3 + 100$ by $n + 10$ using unknown coefficients:

$$\begin{aligned} n^3 + 100 &= (n + 10)\left(n^2 + an + b\right) + c \\ &= n^3 + n^2(10 + a) + n(b + 10a) + 1b + c. \end{aligned}$$

Equating coefficients yields

$$\begin{cases} 10 + a = 0 \\ b + 10a = 0 \\ 10b + c = 100. \end{cases}$$

Solving this system gives $a = -10, b = 100$, and $c = -900$. Therefore,

$$n^3 + 100 = (n + 10)\left(n^2 - 10n + 100\right) - 900.$$

Since $n + 10$ divides itself and $n^3 + 100$, it also divides the remainder, -900. Hence, the maximum possible value of n is when $n + 10 = 900$ or $n = \boxed{890}$.

Polynomial Remainder Theorem

Note that in the previous problem, the remainder when we divide $n^3 + 100$ by $n + 10$ is $(-10)^3 + 100 = -900$. This leads us to the below theorem:

Theorem. If we divide a polynomial $p(x)$ by a linear term $x - a$ for constant a, the remainder is equal to $p(a)$.

Proof. Since $\deg(x - a) = 1$, using the division algorithm,

$$p(x) = (x - a)q(x) + r.$$

In the above expression, r is a constant. Since this equation holds for all values of x, we can plug $x = a$ into the equation. This gives

$$p(a) = (a - a)q(x) + r \implies p(a) = r,$$

as desired.

Fundamental Theorem of Algebra

Theorem. A polynomial $p(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0$ with complex roots $r_1, r_2, r_3, \cdots, r_n$ can be expressed as

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

An alternative phrasing is that every polynomial can be factored into linear and irreducible quadratic terms.

Fundamental Theorem of Algebra

Theorem. A polynomial $p(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0$ with complex roots $r_1, r_2, r_3, \cdots, r_n$ can be expressed as

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

An alternative phrasing is that every polynomial can be factored into linear and irreducible quadratic terms.

Polynomial GCD

The greatest common divisor of two polynomials is the **monic term** (leading coefficient of 1) of largest degree that divides into both polynomials.

Polynomial GCD

The greatest common divisor of two polynomials is the **monic term** (leading coefficient of 1) of largest degree that divides into both polynomials.

For instance, factorizing two polynomials shows that

$$x^4 + 2x^2 - 3 = (x^2 + 3)(x^2 - 1),$$
$$x^5 + 3x^3 = (x^2 + 3)x^3.$$

Therefore, $\gcd(x^4 + 2x^2 - 3, x^5 + 3x^3) = x^2 + 3$.

Example 15. Compute $\gcd(x^4 - x^3, x^3 - x)$.

Computing GCD of two Polynomials

Example. Compute $\gcd(x^4 - x, x^3 - x^2)$.

We factor the two polynomials:

$$x^4 - x = (x^2 - x)(x^2 + x + 1)$$
$$x^3 - x^2 = (x^2 - x)x.$$

Hence, $\gcd(x^4 - x, x^3 - x^2) = x^2 - x$.

Computing GCD of two Polynomials

Example. Compute $\gcd(x^4 - x, x^3 - x^2)$.

We factor the two polynomials:

$$x^4 - x = (x^2 - x)(x^2 + x + 1)$$
$$x^3 - x^2 = (x^2 - x)x.$$

Hence, $\gcd(x^4 - x, x^3 - x^2) = x^2 - x$.

We could also use the division algorithm for polynomials:

$$x^4 - x = \left(x^3 - x^2\right)(x + 1) + \left(x^2 - x\right)$$
$$x^3 - x^2 = \left(x^2 - x\right)x.$$

Therefore, $\gcd(x^4 - x^3, x^3 - x) = x^2 - x$, the final non-zero remainder.

Computing GCD of two Polynomials

Example. Compute $\gcd(x^4 - x, x^3 - x^2)$.

We factor the two polynomials:

$$x^4 - x = (x^2 - x)(x^2 + x + 1)$$
$$x^3 - x^2 = (x^2 - x)x.$$

Hence, $\gcd(x^4 - x, x^3 - x^2) = x^2 - x$.

We could also use the division algorithm for polynomials:

$$x^4 - x = \left(x^3 - x^2\right)(x + 1) + \left(x^2 - x\right)$$
$$x^3 - x^2 = \left(x^2 - x\right)x.$$

Therefore, $\gcd(x^4 - x^3, x^3 - x) = x^2 - x$, the final non-zero remainder.

Euclidean Algorithm for Polynomials

Theorem. If $n(x) = d(x)q(x) + r(x)$ with $\deg(r(x)) < \deg(d(x))$, then

$$\gcd(n(x), d(x)) = \gcd(d(x), r(x)).$$

Euclidean Algorithm for Polynomials

Theorem. If $n(x) = d(x)q(x) + r(x)$ with $\deg(r(x)) < \deg(d(x))$, then

$$\gcd(n(x), d(x)) = \gcd(d(x), r(x)).$$

Extending this method, we can calculate $\gcd(n(x), d(x))$:

$$\begin{aligned}
n(x) &= d(x)q_1(x) + r_1(x) \\
d(x) &= r_1(x)q_2(x) + r_2(x) \\
r_1(x) &= r_2(x)q_3(x) + r_3(x) \\
&\dots \\
r_{n-1}(x) &= r_n(x)q_{n+1}(x) + r_{n+1}(x) \\
r_n(x) &= r_{n+1}(x)q_{n+2}(x).
\end{aligned}$$

Euclidean Algorithm for Polynomials

Theorem. If $n(x) = d(x)q(x) + r(x)$ with $\deg(r(x)) < \deg(d(x))$, then

$$\gcd(n(x), d(x)) = \gcd(d(x), r(x)).$$

Extending this method, we can calculate $\gcd(n(x), d(x))$:

$$\begin{aligned}
n(x) &= d(x)q_1(x) + r_1(x) \\
d(x) &= r_1(x)q_2(x) + r_2(x) \\
r_1(x) &= r_2(x)q_3(x) + r_3(x) \\
&\cdots \\
r_{n-1}(x) &= r_n(x)q_{n+1}(x) + r_{n+1}(x) \\
r_n(x) &= r_{n+1}(x)q_{n+2}(x).
\end{aligned}$$

Then we have

$$\gcd(n(x), d(x)) = \gcd(d(x), r_1(x)) = \gcd(r_1(x), r_2(x)) = \cdots = r_{n+1}(x),$$

the final non-zero remainder.

Polynomial GCD Examples

Example 16. Compute $\gcd(x^5 + 2x^3 + x^2 + x + 1, x^4 + x^2)$.

Example 17. Prove that for natural n the fraction $\frac{21n+4}{14n+3}$ is irreducible. ¶

Example 18. The numbers in the sequence are of the form $a_n = 100 + n^2$:

$$101, 104, 109, 116, 125, 136, 149, 164, 181, 200, 221, \cdots$$

For each positive integer n, let $d_n = \gcd(a_n, a_{n+1})$. Compute the maximum value of d_n. ‖

¶ Source: 1958 IMO

‖ Source: 1985 AIME

GCD of 5th Degree Polynomial

Example. Compute $\gcd(x^5 + 2x^3 + x^2 + x + 1, x^4 + x^2)$.

We use the Euclidean algorithm for polynomials:

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

Therefore, $\gcd(x^5 + 2x^3 + x^2 + x + 1, x^4 + x^2) = \boxed{x^2 + 1}$.

As a check, we can verify that $x = \pm i$ are roots of both equations.

GCD of 5th Degree Polynomial

Example. Compute $\gcd(x^5 + 2x^3 + x^2 + x + 1, x^4 + x^2)$.

We use the Euclidean algorithm for polynomials:

$$x^5 + 2x^3 + x^2 + x + 1 = \left(x^4 + x^2\right)(x) + \left(x^3 + x^2 + x + 1\right)$$

$$x^3 + x^2 + x + 1 = \left(x^2 + 1\right)(x + 1)\,.$$

Therefore, $\gcd(x^5 + 2x^3 + x^2 + x + 1, x^4 + x^2) = \boxed{x^2 + 1}$.

As a check, we can verify that $x = \pm i$ are roots of both equations.

GCD of 5th Degree Polynomial

Example. Compute $\gcd(x^5 + 2x^3 + x^2 + x + 1, x^4 + x^2)$.

We use the Euclidean algorithm for polynomials:

$$\begin{aligned} x^5 + 2x^3 + x^2 + x + 1 &= \left(x^4 + x^2\right)(x) + \left(x^3 + x^2 + x + 1\right) \\ x^4 + x^2 &= \left(x^3 + x^2 + x + 1\right)(x - 1) + \left(x^2 + 1\right) \\ x^3 + x^2 + x + 1 &= \left(x^2 + 1\right)(x + 1). \end{aligned}$$

GCD of 5th Degree Polynomial

Example. Compute $\gcd(x^5 + 2x^3 + x^2 + x + 1, x^4 + x^2)$.

We use the Euclidean algorithm for polynomials:

$$\begin{aligned} x^5 + 2x^3 + x^2 + x + 1 &= \left(x^4 + x^2\right)(x) + \left(x^3 + x^2 + x + 1\right) \\ x^4 + x^2 &= \left(x^3 + x^2 + x + 1\right)(x - 1) + \left(x^2 + 1\right) \\ x^3 + x^2 + x + 1 &= \left(x^2 + 1\right)(x + 1). \end{aligned}$$

Therefore, $\gcd(x^5 + 2x^3 + x^2 + x + 1, x^4 + x^2) = \boxed{x^2 + 1}$.

GCD of 5th Degree Polynomial

Example. Compute $\gcd(x^5 + 2x^3 + x^2 + x + 1, x^4 + x^2)$.

We use the Euclidean algorithm for polynomials:

$$\begin{aligned} x^5 + 2x^3 + x^2 + x + 1 &= \left(x^4 + x^2\right)(x) + \left(x^3 + x^2 + x + 1\right) \\ x^4 + x^2 &= \left(x^3 + x^2 + x + 1\right)(x - 1) + \left(x^2 + 1\right) \\ x^3 + x^2 + x + 1 &= \left(x^2 + 1\right)(x + 1). \end{aligned}$$

Therefore, $\gcd(x^5 + 2x^3 + x^2 + x + 1, x^4 + x^2) = \boxed{x^2 + 1}$.

As a check, we can verify that $x = \pm i$ are roots of both equations.

First IMO Problem Ever

Example. Prove that for natural n the fraction $\frac{21n+4}{14n+3}$ is irreducible.

Using the Euclidean Algorithm for polynomials,

$$\begin{aligned}\gcd(21n+4, 14n+3) &= \gcd(7n+1, 14n+3) \\ &= \gcd(7n+1, 14n+3-2(7n+1)) \\ &= \gcd(7n+1, 1) \\ &= 1.\end{aligned}$$

1985 AIME Sequence

Example. The numbers in the sequence are of the form $a_n = 100+n^2$. For each positive integer n, let $d_n = \gcd(a_n, a_{n+1})$. Compute the maximum value of d_n.

We see that $a_{n+1} - a_n = ((n+1)^2 + 100) - (n^2 + 100) = 2n + 1$.

1985 AIME Sequence

Example. The numbers in the sequence are of the form $a_n = 100+n^2$. For each positive integer n, let $d_n = \gcd(a_n, a_{n+1})$. Compute the maximum value of d_n.

We see that $a_{n+1} - a_n = ((n+1)^2 + 100) - (n^2 + 100) = 2n + 1$.

Therefore, using the Euclidean Algorithm:

$$d_n = \gcd(a_n, a_{n+1}) = \gcd(a_n, a_{n+1} - a_n) = \gcd(n^2 + 100, 2n + 1).$$

Notice that $(2n+1)(2n-1) = 4n^2 - 1$ using difference of squares.

1985 AIME Sequence

Example. The numbers in the sequence are of the form $a_n = 100+n^2$. For each positive integer n, let $d_n = \gcd(a_n, a_{n+1})$. Compute the maximum value of d_n.

We see that $a_{n+1} - a_n = ((n+1)^2 + 100) - (n^2 + 100) = 2n + 1$.

Therefore, using the Euclidean Algorithm:

$$d_n = \gcd(a_n, a_{n+1}) = \gcd(a_n, a_{n+1} - a_n) = \gcd(n^2 + 100, 2n + 1).$$

Notice that $(2n+1)(2n-1) = 4n^2 - 1$ using difference of squares.

Since $d_n \mid n^2 + 100$ and $d_n \mid 2n + 1$, using the linear combination theorem:

$$d_n \mid \left(4\left(n^2 + 100\right) - (2n+1)(2n-1)\right) = 401.$$

1985 AIME Sequence

Example. The numbers in the sequence are of the form $a_n = 100+n^2$. For each positive integer n, let $d_n = \gcd(a_n, a_{n+1})$. Compute the maximum value of d_n.

We see that $a_{n+1} - a_n = ((n+1)^2 + 100) - (n^2 + 100) = 2n + 1$.

Therefore, using the Euclidean Algorithm:

$$d_n = \gcd(a_n, a_{n+1}) = \gcd(a_n, a_{n+1} - a_n) = \gcd(n^2 + 100, 2n + 1).$$

Notice that $(2n+1)(2n-1) = 4n^2 - 1$ using difference of squares.

Since $d_n \mid n^2 + 100$ and $d_n \mid 2n + 1$, using the linear combination theorem:

$$d_n \mid \left(4\left(n^2 + 100\right) - (2n+1)(2n-1)\right) = 401.$$

When $n = 200$, we see $a_{200} = 200^2 + 100 = 40100 = 401 \cdot 100$ and $a_{201} = 201^2 + 100 = 40501 = 401 \cdot 101$. Hence, the maximum possible value of d_n is $\boxed{401}$.