Number Theory

"The queen of mathematics" – Gauss

Peng Shi

Department of Mathematics
Duke University

November 18, 2009

Number Theory has a LOT of Theory

When I think of number theory, the following machineries come to mind

Number Theory has a LOT of Theory

When I think of number theory, the following machineries come to mind

- Congruences and divisibility
- Euler's Theorem
- Chinese remainder
- Order of an element
- Primitive roots
- Quadratic Residues
- Algebraic Field Extensions
- Hensel's Lemma
- Dirichlet Series
- Pell's Equations
- Farey Sequences
- Continued Fractions
- Arithmetic Functions
- Rings and Modules

Number Theory has a LOT of Theory

When I think of number theory, the following machineries come to mind

- Congruences and divisibility
- Euler's Theorem
- Chinese remainder
- Order of an element
- Primitive roots
- Quadratic Residues
- Algebraic Field Extensions
- Hensel's Lemma
- Dirichlet Series
- Pell's Equations
- Farey Sequences
- Continued Fractions
- Arithmetic Functions
- Rings and Modules

We will only cover some of the basic techniques. For information on some of the other techniques, see Naoki Sato's notes, available at `www.artofproblemsolving.com/Resources/Papers/SatoNT.pdf`. (Many of the examples are plagiarized from this source.)

Congruences and divisibility

We say that $a \equiv b \pmod{n}$ if $n | a - b$.
Useful properties:

- If $a \equiv b$ and $c \equiv d \pmod{n}$, then $a - c \equiv b - d \pmod{n}$ and $ac \equiv bd \pmod{n}$.

Congruences and divisibility

We say that $a \equiv b \pmod{n}$ if $n | a - b$.
Useful properties:

- If $a \equiv b$ and $c \equiv d \pmod{n}$, then $a - c \equiv b - d \pmod{n}$ and $ac \equiv bd \pmod{n}$.
- If $n | a$ and $n | b$, then $n | ua + vb$.

Congruences and divisibility

We say that $a \equiv b \pmod{n}$ if $n|a-b$.
Useful properties:

- If $a \equiv b$ and $c \equiv d \pmod{n}$, then $a - c \equiv b - d \pmod{n}$ and $ac \equiv bd \pmod{n}$.
- If $n|a$ and $n|b$, then $n|ua + vb$.
- $\forall n \in \mathbb{Z}$, $n^2 \equiv 0, 1 \pmod{4}$.

Congruences and divisibility

We say that $a \equiv b \pmod{n}$ if $n | a - b$.
Useful properties:

- If $a \equiv b$ and $c \equiv d \pmod{n}$, then $a - c \equiv b - d \pmod{n}$ and $ac \equiv bd \pmod{n}$.
- If $n|a$ and $n|b$, then $n|ua + vb$.
- $\forall n \in \mathbb{Z}$, $n^2 \equiv 0, 1 \pmod{4}$.
- $\forall n \in \mathbb{Z}$, $n^2 \equiv 0, 1, 4 \pmod{4}$. ($0, 1, 4$ are "quadratic residues" mod 8.)

Congruences and divisibility

We say that $a \equiv b \pmod{n}$ if $n|a-b$.
Useful properties:

- If $a \equiv b$ and $c \equiv d \pmod{n}$, then $a-c \equiv b-d \pmod{n}$ and $ac \equiv bd \pmod{n}$.
- If $n|a$ and $n|b$, then $n|ua+vb$.
- $\forall n \in \mathbb{Z}$, $n^2 \equiv 0, 1 \pmod{4}$.
- $\forall n \in \mathbb{Z}$, $n^2 \equiv 0, 1, 4 \pmod{4}$. $(0, 1, 4$ are "quadratic residues" mod 8.)
- If a and b are co-prime, then $\exists u$ such that $au \equiv 1 \pmod{n}$. The "multiplicative inverse" is unique up to equivalence class. Equivalently, $\exists u, v \in \mathbb{Z}$ such that, $au + bv = 1$.

Euler's Theorem

Definition
$\phi(n)$ denotes the number of positive integers less than n and relatively prime to n. This is the Euler's Totient function.

Euler's Theorem

Definition

$\phi(n)$ denotes the number of positive integers less than n and relatively prime to n. This is the Euler's Totient function.

Theorem

If n has prime factors $p_1, \cdots p_k$, then

$$\phi(n) = n \prod_{i=1}^{k} (1 - \frac{1}{p_i})$$

Euler's Theorem

Theorem (Euler's Theorem)

If a is relatively prime to n, then $a^{\phi(n)} \equiv 1 \pmod{m}$.
In particular, if $p \nmid a$, *then* $a^{p-1} \equiv 1 \pmod{p}$ *(Fermat's little theorem).*

Euler's Theorem

Theorem (Euler's Theorem)

If a is relatively prime to n, then $a^{\phi(n)} \equiv 1 \pmod{m}$*.*
In particular, if $p \nmid a$*, then* $a^{p-1} \equiv 1 \pmod{p}$ *(Fermat's little theorem).*

Proof.

Let $a_1, a_2, \cdots, a_{\phi(n)}$ be the positive integers less than n and relatively prime to n. Note that $aa_1, aa_2, \cdots, aa_{\phi(n)}$ is a permultation of these numbers.

Euler's Theorem

Theorem (Euler's Theorem)

If a is relatively prime to n, then $a^{\phi(n)} \equiv 1 \pmod{m}$.
In particular, if $p \nmid a$, then $a^{p-1} \equiv 1 \pmod{p}$ (Fermat's little theorem).

Proof.

Let $a_1, a_2, \cdots, a_{\phi(n)}$ be the positive integers less than n and relatively prime to n. Note that $aa_1, aa_2, \cdots, aa_{\phi(n)}$ is a permultation of these numbers. (This is because $aa_i \equiv aa_j$ implies $a_i \equiv a_j$, so this is an injection of a finite set to itself.)

Euler's Theorem

Theorem (Euler's Theorem)

If a is relatively prime to n, then $a^{\phi(n)} \equiv 1 \pmod{m}$.
In particular, if $p \nmid a$, then $a^{p-1} \equiv 1 \pmod{p}$ (Fermat's little theorem).

Proof.

Let $a_1, a_2, \cdots, a_{\phi(n)}$ be the positive integers less than n and relatively prime to n. Note that $aa_1, aa_2, \cdots, aa_{\phi(n)}$ is a permultation of these numbers. (This is because $aa_i \equiv aa_j$ implies $a_i \equiv a_j$, so this is an injection of a finite set to itself.)
Thus,

$$\begin{aligned} a_1 a_2 \cdots a_{\phi(n)} &\equiv (aa_1)(aa_2)\cdots(aa_{\phi(n)}) \\ &\equiv a^{\phi(n)} a_1 a_2 \cdots a_{\phi(n)} \\ \implies 1 &\equiv a^{\phi(n)} \pmod{n} \end{aligned}$$

$\square$

Chinese Remainder Theorem

Theorem (Chinese Remainder)

If $a_1, a_2, \cdots, a_k$ *are integers and* $m_1, m_2, \cdots, m_k$ *are pairwise relatively prime integers, then the system of congruences*

$$\begin{aligned} x &\equiv a_1 \pmod{m_1} \\ &\vdots \\ x &\equiv a_k \pmod{m_k} \end{aligned}$$

has a unique solution mod $m = m_1 m_2 \cdots m_k$.

Chinese Remainder Theorem

Theorem (Chinese Remainder)

If $a_1, a_2, \cdots, a_k$ are integers and $m_1, m_2, \cdots, m_k$ are pairwise relatively prime integers, then the system of congruences

$$\begin{aligned} x &\equiv a_1 \pmod{m_1} \\ &\vdots \\ x &\equiv a_k \pmod{m_k} \end{aligned}$$

has a unique solution mod $m = m_1 m_2 \cdots m_k$.

Proof.

Since $\frac{m}{m_i}$ is relatively prime to m_i, $\exists t_i$ s.t. $t_i \cdot \frac{m}{m_i} \equiv 1 \pmod{m_i}$. Let $s_i = t_i \cdot \frac{m}{m_i}$.

Chinese Remainder Theorem

Theorem (Chinese Remainder)

If $a_1, a_2, \cdots, a_k$ are integers and $m_1, m_2, \cdots, m_k$ are pairwise relatively prime integers, then the system of congruences

$$\begin{aligned} x &\equiv a_1 \pmod{m_1} \\ &\vdots \\ x &\equiv a_k \pmod{m_k} \end{aligned}$$

has a unique solution mod $m = m_1 m_2 \cdots m_k$.

Proof.

Since $\frac{m}{m_i}$ is relatively prime to m_i, $\exists t_i$ s.t. $t_i \cdot \frac{m}{m_i} \equiv 1 \pmod{m_i}$. Let $s_i = t_i \cdot \frac{m}{m_i}$.
$\forall j \neq i$, $s_i \equiv 0 \pmod{m_j}$, and $s_i \equiv 1 \pmod{m_i}$. Hence, $x = a_1 s_1 + \cdots + a_k s_k$ is a solution.

Chinese Remainder Theorem

Theorem (Chinese Remainder)

If $a_1, a_2, \cdots, a_k$ are integers and $m_1, m_2, \cdots, m_k$ are pairwise relatively prime integers, then the system of congruences

$$\begin{aligned} x &\equiv a_1 \pmod{m_1} \\ &\vdots \\ x &\equiv a_k \pmod{m_k} \end{aligned}$$

has a unique solution mod $m = m_1 m_2 \cdots m_k$.

Proof.

Since $\frac{m}{m_i}$ is relatively prime to m_i, $\exists t_i$ s.t. $t_i \cdot \frac{m}{m_i} \equiv 1 \pmod{m_i}$. Let $s_i = t_i \cdot \frac{m}{m_i}$.
$\forall j \neq i$, $s_i \equiv 0 \pmod{m_j}$, and $s_i \equiv 1 \pmod{m_i}$. Hence,
$x = a_1 s_1 + \cdots + a_k s_k$ is a solution.
To see uniqueness, if x' is another solution, then $x - x' \equiv 0 \pmod{m_i}$ for all i, so $x - x' \equiv 0 \pmod{m}$. $\square$

Chinese Remainder Theorem

Example (From Sunzi Suanjing)

There are certain things whose number is unknown. Repeatedly divided by 3, the remainder is 2; by 5 the remainder is 3; and by 7 the remainder is 2. What will be the (smallest such) number?

Chinese Remainder Theorem

Example (From Sunzi Suanjing)

There are certain things whose number is unknown. Repeatedly divided by 3, the remainder is 2; by 5 the remainder is 3; and by 7 the remainder is 2. What will be the (smallest such) number?

Solution.
$-35 \times 2 + 21 \times 3 + 15 \times 2 = 21.$ □

Chinese Remainder Theorem

Example (From Sunzi Suanjing)

There are certain things whose number is unknown. Repeatedly divided by 3, the remainder is 2; by 5 the remainder is 3; and by 7 the remainder is 2. What will be the (smallest such) number?

Solution.

$-35 \times 2 + 21 \times 3 + 15 \times 2 = 21.$ $\square$

孫子歌 Sunzi Ge

三人同行七十里
五樹梅花廿一枝
七子團圓正月半
一百零五轉回起

Fun with Divisibility

Example

Find all positive integers d such that d divides both n^2+1 and $(n+1)^2+1$ for some integer n.

Fun with Divisibility

Example

Find all positive integers d such that d divides both $n^2 + 1$ and $(n+1)^2 + 1$ for some integer n.

Proof.

Since $(n+1)^2 + 1 = n^2 + 2n + 2$, $d | [n^2 + 2n + 2] - [n^2 + 1] = 2n + 1$

Fun with Divisibility

Example

Find all positive integers d such that d divides both $n^2 + 1$ and $(n+1)^2 + 1$ for some integer n.

Proof.

Since $(n+1)^2 + 1 = n^2 + 2n + 2$, $d | [n^2 + 2n + 2] - [n^2 + 1] = 2n + 1$
So $d | 4n^2 + 4n + 1$

Fun with Divisibility

Example

Find all positive integers d such that d divides both n^2+1 and $(n+1)^2+1$ for some integer n.

Proof.

Since $(n+1)^2+1 = n^2+2n+2$, $d | [n^2+2n+2] - [n^2+1] = 2n+1$
So $d | 4n^2+4n+1$
So $d | 4(n^2+2n+2) - (4n^2+4n+1) = 4n+7$

Fun with Divisibility

Example

Find all positive integers d such that d divides both n^2+1 and $(n+1)^2+1$ for some integer n.

Proof.

Since $(n+1)^2+1 = n^2+2n+2$, $d|[n^2+2n+2]-[n^2+1] = 2n+1$
So $d|4n^2+4n+1$
So $d|4(n^2+2n+2)-(4n^2+4n+1) = 4n+7$
So $d|(4n+7)-2(2n+1) = 5$. So $d|5$. So $d \in \{1,5\}$.

Fun with Divisibility

Example

Find all positive integers d such that d divides both n^2+1 and $(n+1)^2+1$ for some integer n.

Proof.

Since $(n+1)^2+1 = n^2+2n+2$, $d|[n^2+2n+2]-[n^2+1] = 2n+1$
So $d|4n^2+4n+1$
So $d|4(n^2+2n+2)-(4n^2+4n+1) = 4n+7$
So $d|(4n+7)-2(2n+1) = 5$. So $d|5$. So $d \in \{1,5\}$.
Setting $n=2$ shows that both values can be achieved. $\square$

"Big" Results using Little Theorem

Problem

If p is a prime and n is an integer such that $p|(4n^2+1)$ then $p \equiv 1 \pmod 4$.

"Big" Results using Little Theorem

Problem

If p is a prime and n is an integer such that $p|(4n^2+1)$ then $p \equiv 1 \pmod 4$.

Solution.

Clearly, p cannot be 2, so we need to show that $p \not\equiv 3 \pmod 4$. Suppose on the contrary that $p = 4k+3$ for some k. Let $y = 2n$, note that y is relatively prime to p.

By Fermat's Little Theorem,

$$y^{p-1} \equiv 1 \pmod p$$

"Big" Results using Little Theorem

Problem

If p is a prime and n is an integer such that $p|(4n^2+1)$ then $p \equiv 1 \pmod 4$.

Solution.

Clearly, p cannot be 2, so we need to show that $p \not\equiv 3 \pmod 4$. Suppose on the contrary that $p = 4k+3$ for some k. Let $y = 2n$, note that y is relatively prime to p.
By Fermat's Little Theorem,

$$y^{p-1} \equiv 1 \pmod p$$

However, $y^2 \equiv -1 \pmod p$, so

"Big" Results using Little Theorem

Problem

If p is a prime and n is an integer such that $p|(4n^2+1)$ then $p \equiv 1 \pmod 4$.

Solution.

Clearly, p cannot be 2, so we need to show that $p \not\equiv 3 \pmod 4$. Suppose on the contrary that $p = 4k+3$ for some k. Let $y = 2n$, note that y is relatively prime to p.

By Fermat's Little Theorem,

$$y^{p-1} \equiv 1 \pmod p$$

However, $y^2 \equiv -1 \pmod p$, so

$$y^{p-1} \equiv (y^2)^{2k+1} \equiv -1 \pmod p$$

Contradiction. □

Order

If a is relatively prime to n, then let d be the smallest positive integer such that $a^d \equiv 1 \pmod{n}$. We call d the *order* of a modulo m, denoted by $ord_n(a)$.

Order

If a is relatively prime to n, then let d be the smallest positive integer such that $a^d \equiv 1 \pmod{n}$. We call d the *order* of a modulo m, denoted by $ord_n(a)$.

Theorem

If a is relatively prime to n and $a^m \equiv 1 \pmod{n}$, then $ord(a)|m$.

Order

If a is relatively prime to n, then let d be the smallest positive integer such that $a^d \equiv 1 \pmod{n}$. We call d the *order* of a modulo m, denoted by $ord_n(a)$.

Theorem

If a is relatively prime to n and $a^m \equiv 1 \pmod{n}$, then $ord(a)|m$.

Example

Show that the order of 2 modulo 101 is 100.

Order

If a is relatively prime to n, then let d be the smallest positive integer such that $a^d \equiv 1 \pmod{n}$. We call d the *order* of a modulo m, denoted by $ord_n(a)$.

Theorem

If a is relatively prime to n and $a^m \equiv 1 \pmod{n}$, then $ord(a)|m$.

Example

Show that the order of 2 modulo 101 is 100.

Solution.

$ord(2)|\phi(101) = 100$. If $ord(2) < 100$, then either $ord(2)|50$ or $ord(2)|20$.

Order

If a is relatively prime to n, then let d be the smallest positive integer such that $a^d \equiv 1 \pmod{n}$. We call d the *order* of a modulo m, denoted by $ord_n(a)$.

Theorem

If a is relatively prime to n and $a^m \equiv 1 \pmod{n}$, then $ord(a)|m$.

Example

Show that the order of 2 modulo 101 is 100.

Solution.

$ord(2)|\phi(101) = 100$. If $ord(2) < 100$, then either $ord(2)|50$ or $ord(2)|20$.
But it is straightforward to check that $2^{50} \equiv -1$ and $2^{20} \equiv -6 \pmod{101}$. $\square$

Primitive Root

We know that modulo n, $ord(g)|\phi(n)$. We call g a *primitive root* if $ord(g) = \phi(n)$.

Primitive Root

We know that modulo n, $ord(g)|\phi(n)$. We call g a *primitive root* if $ord(g) = \phi(n)$.

Theorem

Positive integer n has a primitive root iff n is one of $2, 4, p^k, 2p^k$, where p is an odd prime.

Primitive Root

We know that modulo n, $ord(g)|\phi(n)$. We call g a *primitive root* if $ord(g) = \phi(n)$.

Theorem

Positive integer n has a primitive root iff n is one of $2, 4, p^k, 2p^k$, where p is an odd prime.

Problem

Show that if p is an odd prime, then the congruence $x^4 \equiv -1 \pmod{p}$ has a solution iff $p \equiv 1 \pmod{8}$.

Solution.

Let $x = g^d$ where g is a primitive root mod p. Then we have $4d \not\equiv 0 \pmod{p-1}$ (since $g^{4d} \not\equiv 1 \pmod{p}$).

Primitive Root

We know that modulo n, $ord(g)|\phi(n)$. We call g a *primitive root* if $ord(g) = \phi(n)$.

Theorem

Positive integer n has a primitive root iff n is one of $2, 4, p^k, 2p^k$, where p is an odd prime.

Problem

Show that if p is an odd prime, then the congruence $x^4 \equiv -1 \pmod{p}$ has a solution iff $p \equiv 1 \pmod{8}$.

Solution.

Let $x = g^d$ where g is a primitive root mod p. Then we have
$4d \not\equiv 0 \pmod{p-1}$ (since $g^{4d} \not\equiv 1 \pmod{p}$).
But $8d \equiv 0 \pmod{p-1}$ (since $g^{8d} \equiv 1 \pmod{p}$).

Primitive Root

We know that modulo n, $ord(g)|\phi(n)$. We call g a *primitive root* if $ord(g) = \phi(n)$.

Theorem

Positive integer n has a primitive root iff n is one of $2, 4, p^k, 2p^k$, where p is an odd prime.

Problem

Show that if p is an odd prime, then the congruence $x^4 \equiv -1 \pmod{p}$ has a solution iff $p \equiv 1 \pmod{8}$.

Solution.

Let $x = g^d$ where g is a primitive root mod p. Then we have
$4d \not\equiv 0 \pmod{p-1}$ (since $g^{4d} \not\equiv 1 \pmod{p}$).
But $8d \equiv 0 \pmod{p-1}$ (since $g^{8d} \equiv 1 \pmod{p}$).
Thus $8|p-1$. □

Another Example

Problem
Show that 2 is a primitive root modulo 3^n for all $n \geq 1$.

Another Example

Problem

Show that 2 is a primitive root modulo 3^n for all $n \geq 1$.

Solution.

Note that $\phi(3^k) = 2 \cdot 3^{k-1}$. It suffices to prove by induction that $\forall k \geq 1$,

$$2^{2 \cdot 3^{k-1}} \equiv 1 + 3^k \pmod{3^{n+1}}$$

Another Example

Problem

Show that 2 is a primitive root modulo 3^n for all $n \geq 1$.

Solution.

Note that $\phi(3^k) = 2 \cdot 3^{k-1}$. It suffices to prove by induction that $\forall k \geq 1$,

$$2^{2\cdot 3^{k-1}} \equiv 1 + 3^k \pmod{3^{n+1}}$$

Induction step:

$$\begin{aligned} & 2^{2\cdot 3^{k-1}} &=& \; 1 + 3^k + 3^{k+1}m \\ \Rightarrow \quad & 2^{2\cdot 3^{k}} &=& \; (1 + 3^k + 3^{k+1}m)^3 \\ & &=& \; 1 + 3^{k+1} + 3^{k+2}M \end{aligned}$$

The result follows. □

Another Example

Problem

Show that 2 is a primitive root modulo 3^n for all $n \geq 1$.

Solution.

Note that $\phi(3^k) = 2 \cdot 3^{k-1}$. It suffices to prove by induction that $\forall k \geq 1$,

$$2^{2\cdot 3^{k-1}} \equiv 1 + 3^k \pmod{3^{n+1}}$$

Induction step:

$$\begin{array}{rrcl} & 2^{2\cdot 3^{k-1}} & = & 1 + 3^k + 3^{k+1}m \\ \Rightarrow & 2^{2\cdot 3^k} & = & (1 + 3^k + 3^{k+1}m)^3 \\ & & = & 1 + 3^{k+1} + 3^{k+2}M \end{array}$$

The result follows. $\square$

In particular, this implies that if $2^n \equiv -1 \pmod{3^k}$, then $3^{k-1} | n$.

One of my Favorite Solutions

Problem

(IMO 1990) Find all positive integers $n > 1$ such that $\frac{2^n+1}{n^2}$ is an integer.

One of my Favorite Solutions

Problem

(IMO 1990) Find all positive integers $n > 1$ such that $\frac{2^n+1}{n^2}$ is an integer.

Solution.

Clearly, n must be odd. Let 3^k be the highest power of 3 deviding n.
Then $3^{2k} | n^2 | 2^n + 1$, $(2^n \equiv -1 \pmod{3^{2k}})$.

One of my Favorite Solutions

Problem
(IMO 1990) Find all positive integers $n > 1$ such that $\frac{2^n+1}{n^2}$ is an integer.

Solution.
Clearly, n must be odd. Let 3^k be the highest power of 3 deviding n. Then $3^{2k}|n^2|2^n+1$, ($2^n \equiv -1 \pmod{3^{2k}}$). By previous slide, this implies $3^{2k-1}|n$.

One of my Favorite Solutions

Problem

(IMO 1990) Find all positive integers $n > 1$ such that $\frac{2^n+1}{n^2}$ is an integer.

Solution.

Clearly, n must be odd. Let 3^k be the highest power of 3 deviding n. Then $3^{2k}|n^2|2^n+1$, ($2^n \equiv -1 \pmod{3^{2k}}$). By previous slide, this implies $3^{2k-1}|n$. So $2k-1 \leq k$, $k \leq 1$. This shows that n has at most one factor of 3. Note that $n = 3$ is a solution. We show that this is the only solution.

One of my Favorite Solutions

Problem

(IMO 1990) Find all positive integers $n > 1$ such that $\frac{2^n+1}{n^2}$ is an integer.

Solution.

Clearly, n must be odd. Let 3^k be the highest power of 3 deviding n. Then $3^{2k}|n^2|2^n+1$, $(2^n \equiv -1 \pmod{3^{2k}})$. By previous slide, this implies $3^{2k-1}|n$. So $2k-1 \le k$, $k \le 1$. This shows that n has at most one factor of 3. Note that $n = 3$ is a solution. We show that this is the only solution.

Suppose that n has a prime factor greater than 3; let p be the least such prime. Then $2^n \equiv -1 \pmod{p}$.

One of my Favorite Solutions

Problem

(IMO 1990) Find all positive integers $n > 1$ such that $\frac{2^n+1}{n^2}$ is an integer.

Solution.

Clearly, n must be odd. Let 3^k be the highest power of 3 deviding n. Then $3^{2k}|n^2|2^n + 1$, ($2^n \equiv -1 \pmod{3^{2k}}$). By previous slide, this implies $3^{2k-1}|n$. So $2k - 1 \leq k$, $k \leq 1$. This shows that n has at most one factor of 3. Note that $n = 3$ is a solution. We show that this is the only solution.

Suppose that n has a prime factor greater than 3; let p be the least such prime. Then $2^n \equiv -1 \pmod{p}$. Let d be the order of 2 modulo p. Since $2^{2n} \equiv 1$, $d|2n$.

One of my Favorite Solutions

Problem

(IMO 1990) Find all positive integers $n > 1$ such that $\frac{2^n+1}{n^2}$ is an integer.

Solution.

Clearly, n must be odd. Let 3^k be the highest power of 3 deviding n. Then $3^{2k}|n^2|2^n + 1$, $(2^n \equiv -1 \pmod{3^{2k}})$. By previous slide, this implies $3^{2k-1}|n$. So $2k - 1 \leq k$, $k \leq 1$. This shows that n has at most one factor of 3. Note that $n = 3$ is a solution. We show that this is the only solution.

Suppose that n has a prime factor greater than 3; let p be the least such prime. Then $2^n \equiv -1 \pmod{p}$. Let d be the order of 2 modulo p. Since $2^{2n} \equiv 1$, $d|2n$. If d is odd, then $d|n$, which implies $2^n \equiv 1$, contradiction. So $d = 2d_1$.

One of my Favorite Solutions

Problem

(IMO 1990) Find all positive integers $n > 1$ such that $\frac{2^n+1}{n^2}$ is an integer.

Solution.

Clearly, n must be odd. Let 3^k be the highest power of 3 deviding n. Then $3^{2k}|n^2|2^n+1$, $(2^n \equiv -1 \pmod{3^{2k}})$. By previous slide, this implies $3^{2k-1}|n$. So $2k-1 \leq k$, $k \leq 1$. This shows that n has at most one factor of 3. Note that $n = 3$ is a solution. We show that this is the only solution.

Suppose that n has a prime factor greater than 3; let p be the least such prime. Then $2^n \equiv -1 \pmod{p}$. Let d be the order of 2 modulo p. Since $2^{2n} \equiv 1$, $d|2n$. If d is odd, then $d|n$, which implies $2^n \equiv 1$, contradiction. So $d = 2d_1$. $2d_1|2n$, so $d_1|n$.

One of my Favorite Solutions

Problem

(IMO 1990) Find all positive integers $n > 1$ such that $\frac{2^n+1}{n^2}$ is an integer.

Solution.

Clearly, n must be odd. Let 3^k be the highest power of 3 deviding n. Then $3^{2k}|n^2|2^n+1$, $(2^n \equiv -1 \pmod{3^{2k}})$. By previous slide, this implies $3^{2k-1}|n$. So $2k-1 \le k$, $k \le 1$. This shows that n has at most one factor of 3. Note that $n = 3$ is a solution. We show that this is the only solution.

Suppose that n has a prime factor greater than 3; let p be the least such prime. Then $2^n \equiv -1 \pmod{p}$. Let d be the order of 2 modulo p. Since $2^{2n} \equiv 1$, $d|2n$. If d is odd, then $d|n$, which implies $2^n \equiv 1$, contradiction. So $d = 2d_1$. $2d_1|2n$, so $d_1|n$.

However, $2d_1 = d|(p-1)$, so $d_1|\frac{p-1}{2}$. This implies $d_1 < p$.

One of my Favorite Solutions

Problem

(IMO 1990) Find all positive integers $n > 1$ such that $\frac{2^n+1}{n^2}$ is an integer.

Solution.

Clearly, n must be odd. Let 3^k be the highest power of 3 deviding n. Then $3^{2k}|n^2|2^n+1$, ($2^n \equiv -1 \pmod{3^{2k}}$). By previous slide, this implies $3^{2k-1}|n$. So $2k-1 \leq k$, $k \leq 1$. This shows that n has at most one factor of 3. Note that $n = 3$ is a solution. We show that this is the only solution.

Suppose that n has a prime factor greater than 3; let p be the least such prime. Then $2^n \equiv -1 \pmod{p}$. Let d be the order of 2 modulo p. Since $2^{2n} \equiv 1$, $d|2n$. If d is odd, then $d|n$, which implies $2^n \equiv 1$, contradiction. So $d = 2d_1$. $2d_1|2n$, so $d_1|n$.

However, $2d_1 = d|(p-1)$, so $d_1|\frac{p-1}{2}$. This implies $d_1 < p$. By minimality $d_1 \in \{1, 3\}$.

One of my Favorite Solutions

Problem

(IMO 1990) Find all positive integers $n > 1$ such that $\frac{2^n+1}{n^2}$ is an integer.

Solution.

Clearly, n must be odd. Let 3^k be the highest power of 3 deviding n. Then $3^{2k}|n^2|2^n+1$, ($2^n \equiv -1 \pmod{3^{2k}}$). By previous slide, this implies $3^{2k-1}|n$. So $2k-1 \leq k$, $k \leq 1$. This shows that n has at most one factor of 3. Note that $n = 3$ is a solution. We show that this is the only solution.

Suppose that n has a prime factor greater than 3; let p be the least such prime. Then $2^n \equiv -1 \pmod{p}$. Let d be the order of 2 modulo p. Since $2^{2n} \equiv 1$, $d|2n$. If d is odd, then $d|n$, which implies $2^n \equiv 1$, contradiction. So $d = 2d_1$. $2d_1|2n$, so $d_1|n$.

However, $2d_1 = d|(p-1)$, so $d_1|\frac{p-1}{2}$. This implies $d_1 < p$. By minimality $d_1 \in \{1, 3\}$. If $d_1 = 1$, then $d = 2$, and $2^2 \equiv 1 \pmod{p}$, contradiction.

One of my Favorite Solutions

Problem

(IMO 1990) Find all positive integers $n > 1$ such that $\frac{2^n+1}{n^2}$ is an integer.

Solution.

Clearly, n must be odd. Let 3^k be the highest power of 3 deviding n. Then $3^{2k}|n^2|2^n+1$, ($2^n \equiv -1 \pmod{3^{2k}}$). By previous slide, this implies $3^{2k-1}|n$. So $2k-1 \leq k$, $k \leq 1$. This shows that n has at most one factor of 3. Note that $n = 3$ is a solution. We show that this is the only solution.

Suppose that n has a prime factor greater than 3; let p be the least such prime. Then $2^n \equiv -1 \pmod{p}$. Let d be the order of 2 modulo p. Since $2^{2n} \equiv 1$, $d|2n$. If d is odd, then $d|n$, which implies $2^n \equiv 1$, contradiction. So $d = 2d_1$. $2d_1|2n$, so $d_1|n$.

However, $2d_1 = d|(p-1)$, so $d_1|\frac{p-1}{2}$. This implies $d_1 < p$. By minimality $d_1 \in \{1, 3\}$. If $d_1 = 1$, then $d = 2$, and $2^2 \equiv 1 \pmod{p}$, contradiction. If $d_1 = 3$, then $d = 6$, and $2^6 \equiv 1 \pmod{p}$, so $p|63$, which implies $p = 7$.

One of my Favorite Solutions

Problem

(IMO 1990) Find all positive integers $n > 1$ such that $\frac{2^n+1}{n^2}$ is an integer.

Solution.

Clearly, n must be odd. Let 3^k be the highest power of 3 deviding n. Then $3^{2k}|n^2|2^n+1$, ($2^n \equiv -1 \pmod{3^{2k}}$). By previous slide, this implies $3^{2k-1}|n$. So $2k-1 \leq k$, $k \leq 1$. This shows that n has at most one factor of 3. Note that $n = 3$ is a solution. We show that this is the only solution.

Suppose that n has a prime factor greater than 3; let p be the least such prime. Then $2^n \equiv -1 \pmod{p}$. Let d be the order of 2 modulo p. Since $2^{2n} \equiv 1$, $d|2n$. If d is odd, then $d|n$, which implies $2^n \equiv 1$, contradiction. So $d = 2d_1$. $2d_1|2n$, so $d_1|n$.

However, $2d_1 = d|(p-1)$, so $d_1|\frac{p-1}{2}$. This implies $d_1 < p$. By minimality $d_1 \in \{1, 3\}$. If $d_1 = 1$, then $d = 2$, and $2^2 \equiv 1 \pmod{p}$, contradiction. If $d_1 = 3$, then $d = 6$, and $2^6 \equiv 1 \pmod{p}$, so $p|63$, which implies $p = 7$. But the order of 2 modulo 7 is 3, which is odd, contradiction. □

Ad hoc techniques

Often times the solution of a number theory problem does not involve heavy machinery, but use other "ad-hoc" ideas. Here's an example.

Ad hoc techniques

Often times the solution of a number theory problem does not involve heavy machinery, but use other "ad-hoc" ideas. Here's an example.

Problem

Show that for any positive integer N, there exists a multiple of N that consists only of 1*s and* 0*s. Furthermore, if N is relative prime to* 10*, show that there exists a multiple that consists only of* 1*s.*

Any ideas?

Ad hoc techniques

Often times the solution of a number theory problem does not involve heavy machinery, but use other "ad-hoc" ideas. Here's an example.

Problem

Show that for any positive integer N, there exists a multiple of N that consists only of 1s and 0s. Furthermore, if N is relative prime to 10, show that there exists a multiple that consists only of 1s.

Any ideas?

Pigeonhole Principle!

Ad hoc techniques

Often times the solution of a number theory problem does not involve heavy machinery, but use other "ad-hoc" ideas. Here's an example.

Problem

Show that for any positive integer N, there exists a multiple of N that consists only of 1s and 0s. Furthermore, if N is relative prime to 10, show that there exists a multiple that consists only of 1s.

Any ideas?

Pigeonhole Principle!

Solution.

Consider the $N+1$ integers 1, 11, 111, $\cdots$, $111\cdots1$ ($N+1$ 1s). When divided by N they leave $N+1$ remainders.

Ad hoc techniques

Often times the solution of a number theory problem does not involve heavy machinery, but use other "ad-hoc" ideas. Here's an example.

Problem

Show that for any positive integer N, there exists a multiple of N that consists only of 1s and 0s. Furthermore, if N is relative prime to 10, show that there exists a multiple that consists only of 1s.

Any ideas?

Pigeonhole Principle!

Solution.

Consider the $N+1$ integers 1, 11, 111, $\cdots$, $111\cdots1$ ($N+1$ 1s). When divided by N they leave $N+1$ remainders. By the pigeonhold principle, two of these remainders are equal, so the difference in the corresponding integer is divisible by N. But the difference is of the form 111...000.
If N is relatively prime to 10, then we can divide out all powers of 10, to obtain an integer of the form 11...1. $\square$

Ad hoc techniques

The following problem illustrates that cleverness trumps heavy machinery.

Problem

(IMO 1988) Let a and b be two positive integers such that $ab+1|a^2+b^2$. Show that $\frac{a^2+b^2}{ab+1}$ is a perfect square.

Ad hoc techniques

The following problem illustrates that cleverness trumps heavy machinery.

Problem

(IMO 1988) Let a and b be two positive integers such that $ab+1 | a^2+b^2$. Show that $\frac{a^2+b^2}{ab+1}$ is a perfect square.

Solution.

Let k be the ratio. If $a=b$ then $2a=k(a^2+1)$.

Ad hoc techniques

The following problem illustrates that cleverness trumps heavy machinery.

Problem

(IMO 1988) Let a and b be two positive integers such that $ab+1 | a^2+b^2$. Show that $\frac{a^2+b^2}{ab+1}$ is a perfect square.

Solution.

Let k be the ratio. If $a=b$ then $2a = k(a^2+1)$. This implies $a=b=k=1$.

Ad hoc techniques

The following problem illustrates that cleverness trumps heavy machinery.

Problem

(IMO 1988) Let a and b be two positive integers such that $ab+1|a^2+b^2$. Show that $\frac{a^2+b^2}{ab+1}$ is a perfect square.

Solution.

Let k be the ratio. If $a=b$ then $2a=k(a^2+1)$. This implies $a=b=k=1$.

If $a<b$, then let (a,b) be a solution of $k(ab+1)=a^2+b^2$ with the smallest $\min\{a,b\}$. Note that b satisfies the quadratic

$$b^2-kab+a^2-k=0$$

Ad hoc techniques

The following problem illustrates that cleverness trumps heavy machinery.

Problem

(IMO 1988) Let a and b be two positive integers such that $ab+1|a^2+b^2$. Show that $\frac{a^2+b^2}{ab+1}$ is a perfect square.

Solution.

Let k be the ratio. If $a=b$ then $2a=k(a^2+1)$. This implies $a=b=k=1$.

If $a<b$, then let (a,b) be a solution of $k(ab+1)=a^2+b^2$ with the smallest $\min\{a,b\}$. Note that b satisfies the quadratic

$$b^2-kab+a^2-k=0$$

Note that $ka-b$ is the other root of this quadratic, and it is also an integer (It is straightforward to show that $ka-b>0$.)

Ad hoc techniques

The following problem illustrates that cleverness trumps heavy machinery.

Problem

(IMO 1988) Let a and b be two positive integers such that $ab + 1 | a^2 + b^2$. Show that $\frac{a^2+b^2}{ab+1}$ is a perfect square.

Solution.

Let k be the ratio. If $a = b$ then $2a = k(a^2 + 1)$. This implies $a = b = k = 1$.

If $a < b$, then let (a, b) be a solution of $k(ab + 1) = a^2 + b^2$ with the smallest $\min\{a, b\}$. Note that b satisfies the quadratic

$$b^2 - kab + a^2 - k = 0$$

Note that $ka - b$ is the other root of this quadratic, and it is also an integer (It is straightforward to show that $ka - b > 0$.) Hence, $(a', b') = (ka - b, a)$ also satisfies $k(a'b' + 1) = a'^2 + b'^2$.

Ad hoc techniques

The following problem illustrates that cleverness trumps heavy machinery.

Problem

(IMO 1988) Let a and b be two positive integers such that $ab+1|a^2+b^2$. Show that $\frac{a^2+b^2}{ab+1}$ is a perfect square.

Solution.

Let k be the ratio. If $a=b$ then $2a=k(a^2+1)$. This implies $a=b=k=1$.

If $a<b$, then let (a,b) be a solution of $k(ab+1)=a^2+b^2$ with the smallest $\min\{a,b\}$. Note that b satisfies the quadratic

$$b^2-kab+a^2-k=0$$

Note that $ka-b$ is the other root of this quadratic, and it is also an integer (It is straightforward to show that $ka-b>0$.) Hence, $(a',b')=(ka-b,a)$ also satisfies $k(a'b'+1)=a'^2+b'^2$.

But $ka-b=\frac{a^2-k}{b}<a$. This contradicts the choice (a,b). $\square$

Conclusion

When you come upon a number theory problem, do not despair:

- Try small cases to get intuition.

Conclusion

When you come upon a number theory problem, do not despair:

- Try small cases to get intuition.
- Consider modulo some prime p and try to apply the theory of congruences.

Conclusion

When you come upon a number theory problem, do not despair:

- Try small cases to get intuition.
- Consider modulo some prime p and try to apply the theory of congruences.
- Consider concepts such as order or primitive root.

Conclusion

When you come upon a number theory problem, do not despair:

- Try small cases to get intuition.
- Consider modulo some prime p and try to apply the theory of congruences.
- Consider concepts such as order or primitive root.
- Be random and try something creative!

Conclusion

When you come upon a number theory problem, do not despair:

- Try small cases to get intuition.
- Consider modulo some prime p and try to apply the theory of congruences.
- Consider concepts such as order or primitive root.
- Be random and try something creative!

Conclusion

When you come upon a number theory problem, do not despair:

- Try small cases to get intuition.
- Consider modulo some prime p and try to apply the theory of congruences.
- Consider concepts such as order or primitive root.
- Be random and try something creative!

Course Logistics: This is the last lecture of this course. Next week is thanksgiving, and the week after that (our final class) is a Putnam practice session.

Conclusion

When you come upon a number theory problem, do not despair:

- Try small cases to get intuition.
- Consider modulo some prime p and try to apply the theory of congruences.
- Consider concepts such as order or primitive root.
- Be random and try something creative!

Course Logistics: This is the last lecture of this course. Next week is thanksgiving, and the week after that (our final class) is a Putnam practice session.

Mark your calendars: The Putnam contest will take place Saturday Dec. 5 from 10am-1pm, from 3pm-6pm. This is MANDATORY for everyone enrolled in the class. We need YOU to help keep our pizza fund alive!

Conclusion

When you come upon a number theory problem, do not despair:

- Try small cases to get intuition.
- Consider modulo some prime p and try to apply the theory of congruences.
- Consider concepts such as order or primitive root.
- Be random and try something creative!

Course Logistics: This is the last lecture of this course. Next week is thanksgiving, and the week after that (our final class) is a Putnam practice session.

Mark your calendars: The Putnam contest will take place Saturday Dec. 5 from 10am-1pm, from 3pm-6pm. This is MANDATORY for everyone enrolled in the class. We need YOU to help keep our pizza fund alive!

Thanks to everyone who attended our talks! We hope that this course was helpful in making you a better problem solver!