Number Theory Techniques

Math 96

October 7th

Announcements

- Homework 2 due by email (dakane@ucsd.edu)
- Homework 3 on course webpage. Due next week.
- If you have not already registered to take the Putnam please do so at: https://www.maa.org/math-competitions/putnam-competition
- If you have not completed either of the first two homeworks, please talk to me after class to ensure a certification of commencement of academic activity.

Number Theory

Number theory is the study of the natural numbers: 1,2,3,… and particular of their arithmetic.

- How do natural numbers add or multiply to get other natural numbers?
- Which polynomials have natural number solutions?

Primes

Definition: A positive integer more than 1 is prime if it cannot be written as the product of two smaller positive integers.

Primes

Definition: A positive integer more than 1 is prime if it cannot be written as the product of two smaller positive integers.

So 101 is prime, but 102 = 2x51 is not.

Fundamental Theorem of Arithmetic

Theorem: Any positive integer n can be written as a product of primes. Furthermore, this product is unique up to reordering of the terms.

Fundamental Theorem of Arithmetic

Theorem: Any positive integer n can be written as a product of primes. Furthermore, this product is unique up to reordering of the terms.

For example, 60 = 2 x 2 x 3 x 5 = 5 x 2 x 3 x 2. But it cannot be written as a product of primes except as two 2s, a 3 and a 5.

Consequence

This means that multiplicatively, a positive integer can be thought of as a bag of primes to be multiplied together. Two integers are the same if and only if they correspond to the same bag of primes.

Consequence

This means that multiplicatively, a positive integer can be thought of as a bag of primes to be multiplied together. Two integers are the same if and only if they correspond to the same bag of primes.

This is useful if you want to think about numbers only considering their multiplication.

Other Basic Concepts

- We say that m divides n (or n is a multiple of m, denoted m|n) if n = axm for some integer a. This happens if and only if every prime dividing m also divides n at least as many times.

Other Basic Concepts

- We say that m divides n (or n is a multiple of m, denoted m|n) if n = axm for some integer a. This happens if and only if every prime dividing m also divides n at least as many times.
- The greatest common divisor of m and n (gcd(n,m)) is the largest integer that divides both. You can get it by taking the product of all the primes that divide both.

Euclidean Algorithm

A more efficient way to compute the gcd of two numbers is by what is known as the Euclidean Algorithm.

Euclidean Algorithm

A more efficient way to compute the gcd of two numbers is by what is known as the Euclidean Algorithm.

It is not hard to see that

gcd(n,m) = gcd(n-m,m) = gcd(n,m-n).

Euclidean Algorithm

A more efficient way to compute the gcd of two numbers is by what is known as the Euclidean Algorithm.

It is not hard to see that

gcd(n,m) = gcd(n-m,m) = gcd(n,m-n).

You can repeatedly subtract the smaller number from the larger one until they are the same.

Example

gcd(255, 374) =

Example

gcd(255, 374) =

gcd(255, 119) =

Example

gcd(255, 374) =

gcd(255, 119) =

gcd(136, 119) =

Example

gcd(255, 374) =

gcd(255, 119) =

gcd(136, 119) =

gcd(17, 119) =

Example

gcd(255, 374) =

gcd(255, 119) =

gcd(136, 119) =

gcd(17, 119) =

gcd(17, 119-6x17) =

Example

gcd(255, 374) =

gcd(255, 119) =

gcd(136, 119) =

gcd(17, 119) =

gcd(17, 119-6x17) =

gcd(17,17) =

Example

gcd(255, 374) =

gcd(255, 119) =

gcd(136, 119) =

gcd(17, 119) =

gcd(17, 119-6x17) =

gcd(17,17) =

17.

Problem

2002 A5: Define a sequence by $a_0 = 1$, together with the rules that $a_{2n+1}=a_n$ and $a_{2n+2}=a_n+a_{n+1}$ for each integer $n \geq 0$. Prove that every positive rational number appears in the set $\{ a_{n-1} / a_n : n \geq 1\} = \{1/1,1/2,2/1,1/3,3/2,\ldots\}$.

Observation 1

If any positive rational number q is put into reduced for q = x/y, where x and y have no common factors. In particular, gcd(x,y) = 1 (this is known as x and y are relatively prime).

Observation 1

If any positive rational number q is put into reduced for q = x/y, where x and y have no common factors. In particular, gcd(x,y) = 1 (this is known as x and y are relatively prime).

We need to show that for any relatively prime x and y that there is some n so that $a_{n-1} = x$, and $a_n = y$.

Observation 2

Suppose that $(a_{n-1},a_n) = (x,y)$ then:

- $(a_{2n-1},a_{2n}) = (x,x+y)$
- $(a_{2n},a_{2n+1}) = (x+y,y)$

Observation 2

Suppose that $(a_{n-1},a_n) = (x,y)$ then:

- $(a_{2n-1},a_{2n}) = (x,x+y)$
- $(a_{2n},a_{2n+1}) = (x+y,y)$

These are the reverses of the steps used in the Euclidean algorithm!

Proof sketch

Given x and y relatively prime, we can use the Euclidean algorithm so that starting with (x,y) we apply steps of the form:

- $(x,y) \rightarrow (x,y-x)$
- $(x,y) \rightarrow (x-y,y)$

until we reach $(1,1) = (a_0,a_1)$.

Proof sketch

Given x and y relatively prime, we can use the Euclidean algorithm so that starting with (x,y) we apply steps of the form:

- $(x,y) \rightarrow (x,y-x)$
- $(x,y) \rightarrow (x-y,y)$

until we reach $(1,1) = (a_0,a_1)$.

Applying these steps in the opposite order, we can find n so that $(a_{n-1},a_n) = (x,y)$.

Example

(x,y) = (2,5):

(2,5) → (2,3) → (2,1) → (1,1) = (a_0,a_1).

Example

(x,y) = (2,5):

(2,5) → (2,3) → (2,1) → (1,1) = (a_0,a_1).

(1,1) = (a_0,a_1)

(2,1) = (a_2,a_3)

(2,3) = (a_5,a_6)

(2,5) = (a_{11},a_{12})

Modular Arithmetic

Have you noticed that you can determine the last digit of a sum or product of two numbers just by adding or multiplying the two last digits? This gives rise to a kind of “last digit arithmetic” which can be useful. Modular arithmetic is a generalization of this to bases other than 10.

Congruence

Definition: We say that two integers a and b are congruent modulo m for some other integer m (denoted $a \equiv b \pmod{m}$) if a-b is a multiple of m.

Basic Facts

- $\equiv \pmod m$ is an equivalence relation:
  - $a \equiv a \pmod m$
  - $a \equiv b \pmod m$ if and only if $b \equiv a \pmod m$
  - $a \equiv b \pmod m$ and $b \equiv c \pmod m \Rightarrow a \equiv c \pmod m$

Basic Facts

- $\equiv \pmod m$ is an equivalence relation:
  - $a \equiv a \pmod m$
  - $a \equiv b \pmod m$ if and only if $b \equiv a \pmod m$
  - $a \equiv b \pmod m$ and $b \equiv c \pmod m \Rightarrow a \equiv c \pmod m$
- Every integer is congruent modulo m to exactly one of $0,1,2,\ldots,m-1$ (by taking the remainder when dividing by m).

More Basic Facts

- If $a \equiv a' \pmod{m}$ and $b \equiv b' \pmod{m}$ then:
  - $a+b \equiv a'+b' \pmod{m}$
  - $ab \equiv a'b' \pmod{m}$

More Basic Facts

- If $a \equiv a' \pmod{m}$ and $b \equiv b' \pmod{m}$ then:
  - $a+b \equiv a'+b' \pmod{m}$
  - $ab \equiv a'b' \pmod{m}$

This essentially says that you can do arithmetic modulo m. That is you can do arithmetic on numbers only ever caring about results modulo m. This gives rise to the ring $\mathbb{Z}/m$.

Problem

1952 A1: Let

$$f(x) = \sum_{i=0}^{n} a_i x^{n-i}$$

be a polynomial of degree n with integral coefficients. If a_0, a_n and f(1) are all odd, prove that f(x) = 0 has no rational roots.

Observation 1

Suppose that f(x) = 0 has a root at p/q. We have that

$0 = a_0 (p/q)^n + a_1(p/q)^{n-1} + \ldots + a_n$.

Observation 1

Suppose that f(x) = 0 has a root at p/q. We have that

$0 = a_0 (p/q)^n + a_1(p/q)^{n-1} + \ldots + a_n$.

Clearing denominators we have

$0 = a_0 p^n + a_1 p^{n-1} q + \ldots a_{n-1} p q^{n-1} + a_n q^n$.

Observation 2

We can take p and q to be relatively prime, so they are not both even. This means that either:

- p is even and q is odd
- q is even and p is odd
- p and q are both odd

Observation 2

We can take p and q to be relatively prime, so they are not both even. This means that either:

- p is even and q is odd
- q is even and p is odd
- p and q are both odd

In each case we can consider what happens modulo 2.

p even q odd

$a_0 p^n + a_1 p^{n-1} q + \ldots a_{n-1} p q^{n-1} + a_n q^n$

is equivalent modulo 2 to

$a_0 0^n + a_1 0^{n-1} 1 + \ldots a_{n-1} 0 1^{n-1} + a_n 1^n \equiv a_n \equiv 1.$

p even q odd

$a_0 p^n + a_1 p^{n-1} q + \ldots a_{n-1} p q^{n-1} + a_n q^n$

is equivalent modulo 2 to

$a_0 0^n + a_1 0^{n-1} 1 + \ldots a_{n-1} 0 1^{n-1} + a_n 1^n \equiv a_n \equiv 1.$

Thus, there is no solution of this form.

q even p odd

$a_0 p^n + a_1 p^{n-1} q + \ldots a_{n-1} p q^{n-1} + a_n q^n$

is equivalent modulo 2 to

$a_0 1^n + a_1 1^{n-1} 0 + \ldots a_{n-1} 1 0^{n-1} + a_n 0^n \equiv a_0 \equiv 1.$

q even p odd

$a_0 p^n + a_1 p^{n-1} q + \ldots a_{n-1} p q^{n-1} + a_n q^n$

is equivalent modulo 2 to

$a_0 1^n + a_1 1^{n-1} 0 + \ldots a_{n-1} 1 0^{n-1} + a_n 0^n \equiv a_0 \equiv 1.$

Thus, there is no solution of this form.

p, q both odd

$a_0 p^n + a_1 p^{n-1} q + \ldots a_{n-1} p q^{n-1} + a_n q^n$

is equivalent modulo 2 to

$a_0 1^n + a_1 1^{n-1} 1 + \ldots a_{n-1} 1 1^{n-1} + a_n 1^n \equiv$

$a_0 + a_1 + \ldots + a_n \equiv f(1) \equiv 1.$

p, q both odd

$a_0 p^n + a_1 p^{n-1} q + \ldots a_{n-1} p q^{n-1} + a_n q^n$

is equivalent modulo 2 to

$a_0 1^n + a_1 1^{n-1} 1 + \ldots a_{n-1} 1 1^{n-1} + a_n 1^n \equiv$

$a_0 + a_1 + \ldots + a_n \equiv f(1) \equiv 1.$

Thus, there is no solution of this form.

p, q both odd

$a_0 p^n + a_1 p^{n-1} q + \ldots a_{n-1} p q^{n-1} + a_n q^n$

is equivalent modulo 2 to

$a_0 1^n + a_1 1^{n-1} 1 + \ldots a_{n-1} 1 1^{n-1} + a_n 1^n \equiv$

$a_0 + a_1 + \ldots + a_n \equiv f(1) \equiv 1.$

Thus, there is no solution of this form.

Therefore, f has no rational roots.

Modular Inverses

You can multiply numbers modulo m, but when can you divide them?

Modular Inverses

You can multiply numbers modulo m, but when can you divide them?

In particular, given a modulo m, its inverse, $a^{-1} \pmod{m}$ should be some number b so that $ab \equiv 1 \pmod{m}$.

Modular Inverses

This is not always possible. For example you cannot divide by 0. There is also no number b so that $2b \equiv 1 \pmod 4$ because 2b will always be even.

Modular Inverses

This is not always possible. For example you cannot divide by 0. There is also no number b so that $2b \equiv 1 \pmod 4$ because 2b will always be even.

However, if a and m are relatively prime, there will always be a unique inverse of a modulo m.

In particular if m is prime and $a \not\equiv 0 \pmod m$, then a has an inverse mod m.

Problem

1957 B1: Consider the determinant $|a_{ij}|$ of order 100 with $a_{ij} = i \times j$. Prove that if the absolute value of each of the 100! terms in the expansion of this determinant is divided by 101 then the remainder in each case is 1.

Observation 1

What is a term in the determinant?

We take 100 entries that have one from each row and one from each column and multiply them together.

Observation 1

What is a term in the determinant?

We take 100 entries that have one from each row and one from each column and multiply them together.

What is the resulting product?

Writing each $a_{ij} = i \times j$, we get the product of all of the rows times the product of all of the columns.

Observation 1

What is a term in the determinant?

We take 100 entries that have one from each row and one from each column and multiply them together.

What is the resulting product?

Writing each $a_{ij} = i \times j$, we get the product of all of the rows times the product of all of the columns.

Each term gives $(1 \cdot 2 \cdot 3 \cdot \ldots \cdot 100)(1 \cdot 2 \cdot 3 \cdot \ldots \cdot 100)$.

Observation 2

101 is prime.

Observation 2

101 is prime.

Each term in the first part of the product has an inverse in the second part. Rearranging, this product modulo 101 equals:
$(11^{-1})\ (22^{-1})\ (33^{-1})\ldots\ ((100)(100)^{-1}) \equiv 1^{100} \equiv 1.$

Observation 2

101 is prime.

Each term in the first part of the product has an inverse in the second part. Rearranging, this product modulo 101 equals:
$(11^{-1})\ (22^{-1})\ (33^{-1})\ldots\ ((100)(100)^{-1}) \equiv 1^{100} \equiv 1.$

Note: Using similar ideas you can prove Wilson's Theorem, which states that for any prime p that $(p-1)! \equiv -1 \pmod{p}$.

Modular Exponents

What are the powers of 3 modulo 7?

$3^0 = 1$

$3^1 = 3$

$3^2 = 9 \equiv 2$

$3^3 = 27 \equiv 6$

$3^4 = 81 \equiv 4$

$3^5 = 243 \equiv 5$

$3^6 = 729 \equiv 1$

$3^7 = 2187 \equiv 3$

$3^8 = 6561 \equiv 2$

$3^9 = 19683 \equiv 6$

$3^{10} = 59049 \equiv 4$

$3^{11} = 177147 \equiv 5$

Modular Exponents

What are the powers of 3 modulo 7?

$3^0 = 1$

$3^1 = 3$

$3^2 = 9 \equiv 2$

$3^3 = 27 \equiv 6$

$3^4 = 81 \equiv 4$

$3^5 = 243 \equiv 5$

$3^6 = 729 \equiv 1$

$3^7 = 2187 \equiv 3$

$3^8 = 6561 \equiv 2$

$3^9 = 19683 \equiv 6$

$3^{10} = 59049 \equiv 4$

$3^{11} = 177147 \equiv 5$

…and it repeats.

This is not uncommon.

Fermat's Little Theorem

Theorem: Let p be a prime and a be relatively prime to p. Then

$$a^{p-1} \equiv 1 \pmod{p}.$$

Fermat's Little Theorem

Theorem: Let p be a prime and a be relatively prime to p. Then

$$a^{p-1} \equiv 1 \pmod{p}.$$

This also means that $a^k \equiv a^{k+(p-1)} \equiv a^{k+2(p-1)}$. In fact, a^k modulo p will only depend on what k is modulo p-1.

Order of an Element

So the powers of a modulo p repeat every p-1 terms, but they may repeat more often than that.

Order of an Element

So the powers of a modulo p repeat every p-1 terms, but they may repeat more often than that.

We define $\text{ord}_p(a)$ to be the smallest positive integer k so that $a^k \equiv 1 \pmod{p}$. It is not hard to see that the powers of a repeat every $\text{ord}_p(a)$ terms, but only repeat that often.

Order of an Element

So the powers of a modulo p repeat every p-1 terms, but they may repeat more often than that.

We define $\text{ord}_p(a)$ to be the smallest positive integer k so that $a^k \equiv 1 \pmod{p}$. It is not hard to see that the powers of a repeat every $\text{ord}_p(a)$ terms, but only repeat that often.

It must also be the case that $\text{ord}_p(a)$ divides p-1 since $a^{p-1} \equiv a^0 \pmod{p}$.

Primitive Roots

Also, interestingly, modulo every prime p it is possible to find a primitive root. That is some number g modulo p so that $ord_p(g) = p-1$.

Primitive Roots

Also, interestingly, modulo every prime p it is possible to find a primitive root. That is some number g modulo p so that $ord_p(g) = p-1$.

This means that $g, g^2, g^3, \ldots, g^{p-1}$ must be exactly the numbers $1,2,3,\ldots,p-1$ modulo p. That is every number modulo p (except for 0) can be written as a power of g.

Problem

1972 A5: Show that if n is an integer greater than 1, then n does not divide 2^n-1.

Observation 1

Assume for sake of contradiction that $n \mid 2^n - 1$.

Let p be a prime dividing n.

Observation 1

Assume for sake of contradiction that $n \mid 2^n-1$.

Let p be a prime dividing n.

- Since p divides n and n divides 2^n-1, p must divide 2^n-1.
  - Note: p cannot be 2.

Observation 1

Assume for sake of contradiction that $n \mid 2^n-1$.

Let p be a prime dividing n.

- Since p divides n and n divides 2^n-1, p must divide 2^n-1.
  - Note: p cannot be 2.
- $2^n \equiv 1 \pmod{p}$
  - This means that n is a multiple of $\text{ord}_p(2)$.

Observation 2

What if p is the smallest prime dividing n?

Observation 2

What if p is the smallest prime dividing n?

$\text{ord}_p(2)$ must also divide n.

Observation 2

What if p is the <u>smallest</u> prime dividing n?

$\text{ord}_p(2)$ must also divide n.

However, $1 < \text{ord}_p(2) \leq p-1$.

This means that n must have another factor smaller than p.

Observation 2

What if p is the smallest prime dividing n?

$\text{ord}_p(2)$ must also divide n.

However, $1 < \text{ord}_p(2) \leq p-1$.

This means that n must have another factor smaller than p.

Contradiction!