Discrete Mathematics Recitation Class

Tianyu Qiu

University of Michigan - Shanghai Jiaotong University

Joint Institute

Summer Term 2020

Contents

Fermat's Factorication Method

Finding two factors of an odd number

Process:

1. Find the smallest k that $k^2 > n$.
2. Consider successively the numbers $k^2 - n,\ (k+1)^2 - n,\ (k+2)^2 - n, \cdots$ until one of these numbers is a square.
3. The process must terminate, since

$$\left(\frac{n+1}{2}\right)^2 - n = \left(\frac{n-1}{2}\right)^2$$

Application of Fermat's Factorication Method

e.g.
Find two factors of 12345 with the least difference.
Solution

$$111^2 < 12345 < 112^2$$

$$12345 = 3 \times 5 \times 823 = 419^2 - 404^2$$

Last Digits of Squares

1. Last Digit: 0,1,4,5,6,9
2. Last Two Digits: 0, 1, 4, 9, 16, 21, 24, 25, 29, 36, 41, 44, 49, 56, 61, 64, 69, 76, 81, 84, 89, 96

Fermat's Little Theorem

Theorem (Fermat's Little Theorem)

Let $p, a \in \mathbb{N}$. If p is prime and $p \nmid a$, then

$$a^{p-1} \equiv 1 \ (mod\ p)$$

More generally, for any prime $p \in \mathbb{N}$ and $a \in \mathbb{Z}$,

$$a^{p} \equiv a \ (mod\ p)$$

The Converse of Fermat's Little Theorem is not true.

Counterexample

$2^{341-1} \equiv 1 \pmod{341}$, however $341 = 11 \times 31$ is not prime.

Composite numbers of which $a^{p-1} \equiv 1$ (mod p) are called *Fermat pseudoprimes to base a*.

Application of Fermat's Little Theorem

- Finding the modulo of a very large number

$$5^{38} = 5^{10 \cdot 3+8} = (5^10)^3(5^2)^4 \equiv 1^3 \cdot 3^4 \equiv 81 \equiv 4 \pmod{11}$$

- Showing that a number n is not prime
  Base on the fact that if for some

$$a \in \mathbb{N} \setminus \{0\},\ a^n \not\equiv a \pmod{\mathrm{n}}$$

  then n is not prime.
  e.g.
  $2^{117} \not\equiv 2 \pmod{117}$, then 117 is not prime.

Fermat's Little Theorem

Lemma

Let $p, q \in \mathbb{N} \setminus \{0\}$ *be primes such that*

$$a^p \equiv a \ (mod\ q) \qquad and \qquad a^q \equiv a \ (mod\ p)$$

then

$$a^{pq} \equiv pq \quad (mod\ pq)$$

Wilson's Theorem

Theorem (Wilson's Theorem)

Let $p \in \mathbb{N}$ be prime, then

$$(p-1)! \equiv -1 \pmod{p}$$

Classification of Algorithms

- By Function
  1. Sorting Algorithm:
     - Binary Sort
     - Insertion Sort
     - Selection Sort
     - Merge Sort
     - Quick Sort
  2. Searching Algorithm:
     - Linear Search
     - Binary Search
- By Form
  - Recursive Algorithm
  - Iterative Algorithm

Landau Symbol

Definitions:

1. *big oh* (O): Let A be $\mathbb{R}$ or $\mathbb{N}$. Let $f : A \longrightarrow \mathbb{R}$ and $g : A \longrightarrow \mathbb{R}$. We say f is $O(g)$, pronounced "f is big-oh of g'', if there exists $k, C \in \mathbb{N}$ such that for all $x \in A$ with $x > k, |f(x)| \leq C|g(x)|$. We call O the Landau symbol big-oh.
2. *big omega* (Ω): If g is $O(f)$, then f is $\Omega(g)$.
3. *big theta* (Θ): If f is $O(g)$ and f is $\Omega(g)$, then f is $\Theta(g)$.

Theorem

Let $f : \mathbb{N} \longrightarrow \mathbb{R}$ and $g : \mathbb{N} \longrightarrow \mathbb{R}$. If there exists $C \in \mathbb{R}$ with $C \geq 0$ such that

$$\lim_{n \to \infty} \frac{|f(n)|}{|g(n)|} = C$$

then f is $O(g)$.

Landau Symbol

Theorem

$\ln(n!)$ *is order* $n \ln(n)$

Theorem

Let $n \in \mathbb{N} \setminus \{0\}$. *If* $f : \mathbb{R} \longrightarrow \mathbb{R}$ *is a polynomial of degree* n, *then* f *is order* x^n.

Theorem

Let $p, q \in \mathbb{R}$ *with* $0 < p < q$. *Then* n^q *is not* $O(n^p)$

Theorem

n *is not* $O(\ln(n))$

Exercise 2.1

Let $(\mathbb{N}, \text{succ})$ be a realization of the natural numbers with successor function succ. We define addition of the numbers 0 and $1 := \mathit{succ}(0)$ by setting

$$n + 0 := n, \qquad n + 1 := \mathit{succ}(n), n \in \mathbb{N}$$

i) Formulate an inductive deffinition for $n + m$, where $m, n \in \mathbb{N}$.
ii) Set $2 := \mathit{succ}(1),\ 3 := \mathit{succ}(2),\ 4 := \mathit{succ}(3)$. Verify that

$$2 + 2 = 4$$

iii) Prove by induction that

$$n + m = m + n$$

Solutions

Cited from Chenyan Zhang

i) Inductive Definition: For $m, n \in \mathbb{N}$

$$n + succ(m) = succ(n + m)$$

ii)

$$2+2 = succ(2+1) = succ(succ(2+0)) = succ(succ(2)) = succ(3) = 4$$

iii)

1. Prove Associativity: Apply induction
   Suppose $(a + b) + c = a + (b + c)$, then for $succ(c) \cdots$
2. Prove Communicativity: Apply induction twice
   Prove that $n + 0 = 0 + n$, then prove that $m + n = n + m$

Exercise 2.3

Prove that the induction axiom implies the well-ordering principle.

Solutions

Cited from Chenyan Zhang

Let $m \in \mathbb{N}$, define S_m to be the set that contains m and the successor of any elements in S_m. By induction axiom, $S_0 = \mathbb{N}$.

Define $A := \{m : S \subset S_m\}$, where $S \subset \mathbb{N}$ is nonempty. Then $S \subset S_0 = \mathbb{N}$, i.e. $0 \in A$.

Assume that $\forall_{m \in A}\, succ(m) \in A$, since $0 \in A$, by induction axiom, $A = \mathbb{N}$. Since S is nonempty, suppose $m_0 \in S$. We obtain that $m_0 \notin S_{succ(m_0)}$, thus $succ(m_0) \notin A$. Thus $A \neq \mathbb{N}$, which leads to contradiction.

Thus our assumption is false, we obtain $\exists_{m \in A}\, succ(m) \notin A$. Since $succ(m) \notin A$, then $S \not\subset S_{succ(m)}$ and S_m for this m.

It means that $\exists_{m' \in S} \notin S_{succ(m)}$ and $\forall_{m'' \in S}\, m'' \in S_m$.

$m' \in S_m, m' \notin S_{succ(m)}$. Since $S_m \setminus S_{succ(m)} = \{m\}$, $m' = m$. Since $m' \in S$, thus $m \in S$, m is the least element of S. In conclusion,

$$\forall_{S \subset \mathbb{N}} \ \exists_{m \in S} \ S \in S_m$$

Exercise 3.3

Let

$$m \sim n :\Leftrightarrow 2 \mid (n - m), \;\; m, n \in \mathbb{Z}$$

i) Show that $\sim$ is an equivalence relation.
ii) What partition $\mathbb{Z}_2 := \mathbb{Z}/\sim$ is induced by $\sim$?
iii) Define addition and multiplication on $\mathbb{Z}_2$ by the addition and multiplication of class representatives, i.e.

$$[m] + [n] := [m + n], \qquad [m] \cdot [n] := [m \cdot n]$$

Show that these operations are well-defined, i.e. independent of the representatives m and n of each classes.
iv) Show that $(\mathbb{Z}_2, +, \cdot)$ is a field.

Solutions

i) Since $\sim$ is reflexive, symmetric and transitive, it is an equivalence relation.
ii) $[0]_2$ and $[1]_2$.
iii) For arbitrarily chosen $m, n \in [0]_2; p, q \in [1]_2$, check

$$[m+n]_2, [m+p]_2, [p+q]_2, [mp]_2, [mn]_2, [pq]_2$$

iv)

1. Check $(\mathbb{Z}_2, +)$ is an abelian group.
2. Check existence of unique multiplicative unit element
3. Check associativity, communicativity and distributivity.
4. Check additive unit element is not equal to multiplicative unit element.
5. Check existence of unique multiplicative inverse element.

Exercise 3.10

Let D be the set of all primes of the form $4 \cdot n + 3$ for $n \in \mathbb{N}$. We suppose D to be finite and define $d = 4 \cdot (3 \cdot 7 \cdot \cdots \cdot p) - 1$, where p is the largest prime in D.

i) Prove that no prime of the form $4 \cdot k + 3$ divides d.

ii) Prove that d is not divisible by $4 \cdot k + 1$.

iii) Conclude that there is an infinite number of primes of the form $4 \cdot n + 3$.

Solutions

i) Since each prime $q \in D$ has the property that $q|(d+1)$. Since d and $d+1$ are relatively prime. Thus $q \nmid d$, which completes the proof. More generally, no odd numbers in the form of $4 \cdot k + 3$ (except d itself) divides d.
ii) If d is prime, then no $4 \cdot k + 1$(except 1) divides d. If d is Composite, then according to the conclusion of i), we obtain that d can only have factors in the form of $4 \cdot k + 1$. However, we have that $([1]_4)^n \equiv [1]_4 \not\equiv [3]_d \equiv [d]_4$. So it leads to contradiction. Thus d cannot be a composite, which completes the proof.
iii) We can contruct the sequence of SOME primes of the form $4 \cdot k + 3$ in the following way:

$$a_1 := 3, a_2 := 7, \qquad a_{n+1} := 4 \cdot \left(\prod_{i=1}^{n} a_n \right) - 1$$

This sequence is definitely infinite, which completes the proof.