Introduction to Number Theory

Part A.

- Preliminary
- Divisibility

Nikenasih B, M.Si
Mathematics Educational Department
Faculty of Mathematics and Natural Science
State University of Yogyakarta

Contents

- Preliminary
- Divisibility
- Congruence
- Unique Factorisation
- Linear Diophantine Equation
- Arithmetic Functions

Preliminary
1.1 Introduction

Number Theory is one of the oldest and most beautiful branches of Mathematics. It abounds in problems that yet simple to state, are very hard to solve. Some number-theoretic problems that are yet unsolved are:

1. (Goldbach's Conjecture) Is every even integer greater than 2 the sum of distinct primes?
2. (Twin Prime Problem) Are there infinitely many primes *p such that p+2 is also a prime?*
3. Are there infinitely many primes that are 1 more than the square of an integer?
4. Is there always a prime between two consecutive squares of integers?

Preliminary
1.2 Well Ordering

The set N = {0,1,2,3,4, . . .} of natural numbers is endowed with two operations, addition and multiplication, that satisfy the following properties for natural numbers *a*,*b*, and *c*:

1. *Closure*: $a+b$ and ab are also natural numbers.
2. *Associative laws*: $(a+b)+c = a+(b+c)$ and $a(bc) = (ab)c$.
3. *Distributive law*: $a(b+c) = ab+ac$.
4. *Additive Identity*: $0+a = a+0 = a$
5. *Multiplicative Identity*: $1a = a1 = a$.

Preliminary
1.3 Mathematical Induction

Mathematical induction is a method of mathematical proof typically used to establish that a given statement is true for all natural numbers (positive integers).

It is done by proving that the **first** statement in the infinite sequence of statements is true, and then proving that if **any one** statement in the infinite sequence of statements is true, then so is the **next** one.

Example.

Prove that the expression

$$3^{3n+3} - 26n - 27$$

is a multiple of 169 for all natural numbers n.

Solution

For $n = 1$ we are asserting that $36 - 53 = 676 = 169 \cdot 4$ is divisible by 169, which is evident.

Assume the assertion is true for $n-1, n > 1$, i.e., assume that

$3^{3n} - 26n - 1 = 169N$ for some integer N. Then

$3^{3n+3} - 26n - 27 = 27 \cdot 3^{3n} - 26n - 27$

$= 27(3^{3n} - 26n - 1) + 676$

which reduces to

$27 \cdot 169N + 169 \cdot 4n$,

which is divisible by 169.

The assertion is thus established by induction.

Problems

- Prove that $11^{n+2}+12^{2n+1}$ *is divisible by 133 for* all natural numbers *n*.

- Prove that the sum of the cubes of three consecutive positive integers is divisible by 9.

Preliminary
1.4 Pigeon Hole Principal (PHP)

- The Pigeonhole Principle states that if *n+1 pigeons fly to n holes, there must be a pigeonhole containing at least two pigeons.*

- This apparently trivial principle is very powerful. Let us see some examples.

Example

- If there is 101 mails which will be inserted on mail box, prove that at least there exist one mail box contains at least 3 mails.

- Solution :

  Jika seluruh kotak pos maksimal hanya berisi 2 surat, maka jumlah maksimal surat yang dapat masuk kotak pos adalah 100. Tetapi jumlah surat yang ada yaitu 101. Maka dapat dipastikan ada sedikitnya satu kotak pos berisi sekurang-kurangnya 3 surat.

Example

Let A be any set of twenty integers chosen from the arithmetic progression 1,4, . . . ,100. Prove that there must be two distinct integers in A whose sum is 104.

Solution: We partition the thirty four elements of this progression into eighteen groups {1},{52}, {4,100} , {7,97}, {10,94}, . . . {49,55}. Since we are choosing twenty integers and we have eighteen sets, by the Pigeonhole Principle there must be two integers that belong to one of the pairs, which add to 104.

Exercises

- Pada sebuah pesta setiap orang yang hadir diharuskan membawa permen. Jika pada pesta tersebut jumlah orang yang hadir ada 10 sedangkan jumlah permen yang ada sebanyak 50 buah, buktikan bahwa ada sekurang-kurangnya 2 orang yang membawa permen dalam jumlah yang sama.

- Jika terdapat $n^2 + 1$ titik yang terletak di dalam sebuah persegi dengan panjang sisi n, buktikan bahwa ada sekurang-kurangnya 2 titik yang memiliki jarak tidak lebih dari $\sqrt{2}$ satuan.

- *Titik letis pada bidang adalah titik yang mempunyai koordinat berupa pasangan bilangan bulat.* Misalkan P^1, P^2, P^3, P^4, P^5 adalah lima titik letis berbeda pada bidang. Buktikan bahwa terdapat sepasang titik (P^i, P^j), $i \neq j$, demikian, sehingga ruas garis P^iP^j memuat sebuah titik letis selain P^i dan P^j.

Jika terdapat $n^2 + 1$ titik yang terletak di dalam sebuah persegi dengan panjang sisi n, buktikan bahwa ada sekurang-kurangnya 2 titik yang memiliki jarak tidak lebih dari $\sqrt{2}$ satuan.

jawab :

Bagi persegi tersebut menjadi persegi kecil dengan panjang sisi 1 satuan. Akibatnya, terdapat n^2 persegi kecil. Karena terdapat $n^2 + 1$ titik yang terletak pada n^2 persegi, maka menurut PHP minimal terdapat 2 titik yang terletak pada 1 tempat. Jarak maksimal dua titik pada persegi 1 satuan adalah $\sqrt{2}$ satuan. Jadi, terbukti ada sekurang-kurangnya 2 titik yang memiliki jarak tidak lebih dari $\sqrt{2}$ satuan.

Titik letis pada bidang adalah titik yang mempunyai koordinat berupa pasangan bilangan bulat. Misalkan P^1, P^2, P^3, P^4, P^5 adalah lima titik letis berbeda pada bidang. Buktikan bahwa terdapat sepasang titik (P^i, P^j), $i \neq j$, demikian, sehingga ruas garis P^iP^j memuat sebuah titik letis selain P^i dan P^j.

Jawab :

Kombinasi yang mungkin untuk titik letis dilihat dari ganjil/genap absis atau ordinatnya adalah (ganjil, ganjil), (ganjil, genap), (genap, ganjil) dan (genap, genap). Karena terdapat 5 titik letis, akibatnya minimal terdapat dua titik yang mempunyai jenis yang sama dan ruas garis yang dibentuk oleh kedua titik tersebut pasti memuat titik letis.

(ganjil + ganjil) / 2 pasti bilangan bulat.

(genap + genap) / 2 pasti bilangan bulat.

Divisibility
Division Algorithm

For every a and b positive integers, then there exist c dan r unique nonnegative integers such that a can be stated as

$$a = (b \times c) + r$$

or

$$a = bc + r$$

where $0 \leq r < b$.

Divisibility

For examples

1. b = 3, a = 8, then c = 2, r = 2
2. b = 7, a = 23, then c = 3, r = 2
3. b = 4, a = 51, then c = 12, r = 3
4. b = 5, a = 25, then c = 5, r = 0

Divisibility
Divisors (r = 0)

DEF: Let a, b and c be integers such that

$$a = b \cdot c \ .$$

Then b and c are said to ***divide*** (or are ***factors***) of a, while a is said to be a ***multiple*** of b (as well as of c). The pipe symbol "|" denotes "divides" so the situation is summarized by:

$$b \mid a \ \wedge \ c \mid a \ .$$

NOTE: Students find notation confusing, and think of "|" in the reverse fashion, perhaps confuse pipe with forward slash "/"

Divisibility
Divisors. Examples

Q: Which of the following is true?

1. $77 \mid 7$
2. $7 \mid 77$
3. $24 \mid 24$
4. $0 \mid 24$
5. $24 \mid 0$

Divisibility
Divisors. Examples

A:

1. $77 \mid 7$: false bigger number can't divide smaller positive number
2. $7 \mid 77$: true because $77 = 7 \cdot 11$
3. $24 \mid 24$: true because $24 = 24 \cdot 1$
4. $0 \mid 24$: false, only 0 is divisible by 0
5. $24 \mid 0$: true, 0 is divisible by every number ($0 = 24 \cdot 0$)

Divisibility
Divisor Theorem

THM: Let *a, b,* and *c* be integers. Then:

- *If* b | a *then* b | ac *for every number c.*
- *If* b | a *and* a | c *then* b | c.
- *If* b | a *and* b | c *then* b | ax+cy *for every x,y numbers* .
- *If* b | a *and* a | b *then* $a = \pm b$.
- *If* b | a *and* $b \neq 0$, *then* $|b| \leq |a|$.
- *If* $m \neq 0$, *then b* | a *if and only if* mb | ma.

Try this : if bc | a, then b| a and c | a

Divisibility
Proof of no. 1

In general, such statements are proved by starting from the definitions and manipulating to get the desired results.

EG. *Proof of no. 1* ($b|a \rightarrow b|ac$):

Suppose $b|a$. By definition, there is a number q such that $a = bq$. Multiply both sides by c to get $ac = bqc = b\,(qc)$. Consequently, ac has been expressed as b times the integer qc so by definition of "|", $b|ac$ •

Divisibility
Proof no. 4

- *If* b | a *and* a | b *then* $a = \pm b$.

Jawab :

Diketahui b | a, artinya terdapat d sedemikian sehingga a = bd.

Diketahui pula a | b, artinya terdapat c sedemikian sehingga b = ac.

Substitusikan persamaan pertama ke persamaan kedua, diperoleh

b = (bd) c.

b = bdc

b – bdc = 0

b (1 – dc) = 0

Dua buah bilangan hasil kalinya nol, maka salah satu atau keduanya harus nol. Karena b bukan nol, maka 1 – dc = 0

Darisini diperoleh dc = 1. Nilai yang memenuhi adalah d = c = ± 1.

Jadi, a = $\pm b$.

Let r be the remainder when 1059,1417 and 2312 are divided by $d > 1$. *Find the value of* $d-r$.

Solution : By the Division Algorithm,

$1059 = q1d + r$,

$1417 = q2d + r$,

$2312 = q3d + r$, *for some integers* $q1, q2, q3$.

From this,

$358 = 1417 - 1059 = d(q2 - q1)$,

$1253 = 2312 - 1059 = d(q3 - q1)$ *and*

$895 = 2312 - 1417 = d(q3 - q2)$.

Hence $d|358 = 2 \cdot 179$, $d|1253 = 7 \cdot 179$ *and* $7|895 = 5 \cdot 179$.

Since $d > 1$, *we conclude that* $d - r = 179 - 164 = 15$.

Diketahui bahwa

(i) $(a^n - b^n) = (a - b)(a^{n-1} + a^{n-2}b + a^{n-3}b^2 + \cdots + ab^{n-2} + b^{n-1})$ dengan $n \in$ bilangan asli

(ii) $(a^n + b^n) = (a + b)(a^{n-1} - a^{n-2}b + a^{n-3}b^2 - \cdots - ab^{n-2} + b^{n-1})$ dengan $n \in$ bilangan ganjil

Maka

- $(a - b)$ membagi $(a^n - b^n)$ untuk semua a, b bulat dan n bilangan asli
- $(a + b)$ membagi $(a^n + b^n)$ untuk semua a, b bulat dan n bilangan ganjil

Divisibility
Prime vs composit number

- A *prime number p is a positive integer greater than 1 whose only positive divisors are 1 and p. If the integer n > 1 is not prime, then we say that it is composite.*

- For example, 2, 3, 5, 7, 11, 13, 17, 19 are prime, 4, 6, 8, 9, 10, 12, 14, 15, 16, 18, 20 are composite. The number 1 is neither a prime nor a composite.

- Misalkan M menyatakan perkalian 100 bilangan prima yang pertama. Berapa banyakkah angka 0 di akhir bilangan M?

- Find all the primes of the form $n^3 - 1$, *for integer* $n > 1$.

- Prove that 3 never divides $n^2 + 1$.

References

- Hermanto, Eddy. *Draft Diktat Pembinaan Olimpiade SMA*.

- Santos, David A. *Number theory for mathematical Contest*.