International Baccalaureate

LECTURE NOTES

MATHEMATICS HL – FURTHER MATHEMATICS HL

Christos Nikolaidis

TOPIC
NUMBER THEORY

March 2018

1. METHODS OF PROOF

Consider the statement

If someone lives in Greece then he lives in Europe

The converse of this statement is

If someone lives in Europe then he lives in Greece.

The contrapositive of this statement is

If someone does not live in Europe then he does not live in Greece

We will use this example to demonstrate two kinds of proof.

- **Proof by a counterexample**

A counterexample is enough to establish that a statement is not true in general. For example, let us prove that the converse of the statement above is not true:

If someone lives in Europe, he does not necessarily live in Greece.

Proof: Select a resident of France. He lives in Europe but he does not live in Greece!

- **Proof by contradiction**

The contrapositive of the original statement is true:

If someone does not live in Europe then he does not live in Greece

Proof. Suppose that a person A does not live in Europe.

If A lives in Greece then by the original statement A lives in Europe. Contradiction.

The principle of contradiction is based on the following fact:

If A then B

is equivalent to the contrapositive statement

If not B then not A

Indeed: if not B then not A because if A then B, contradiction!

Let us see two more mathematical examples

EXAMPLE

Let a be an integer. Prove the following statements:

(a) If a^2 is even then a is even.

Proof by contradiction:

Let a^2 be even. If a is odd, then $a=2n+1$ for some integer n. But

$$a^2=(2n+1)^2=4n^2+4n+1=2(2n^2+2n)+1$$

which is odd. Contradiction.

(b) If a^2 is a multiple of n, then a is not necessarily a multiple of n.

Proof by a counterexample:

For $a=6$ and $n=4$,

6^2 is a multiple of 4 but 6 is not a multiple of 4

NOTICE.

We very often do not refer at all to the term "contradiction"; we simply prove the contrapositive statement.

A classical mathematical example is the definition of a 1-1 function: different elements map to different images, that is

$$x_1 \neq x_2 \Rightarrow f(x_1) \neq f(x_2)$$

It is much more practical to use the equivalent statement

$$f(x_1) = f(x_2) \Rightarrow x_1 = x_2$$

This is in fact the contrapositive statement of the definition

---

A classical example of contradiction is the pigeonhole principle presented below.

- **The pigeonhole principle**

Suppose that n+1 pigeons are placed in n pigeonholes

Then, there exists a pigeonhole with at least 2 pigeons

Indeed, is all pigeonholes had at most 1 pigeon we would have at most n pigeons, contradiction.

EXAMPLE

There are 400 people in a club. At least two of them have their birthday on the same day.

Indeed, if all of them had their birthday on different days we would have at most 366 people, contradiction.

A more general form says

Suppose that kn+1 pigeons are placed in n pigeonholes

Then, there exists a pigeonhole with at least k+1 pigeons

Indeed, is all pigeonholes had at most k pigeons we would have at most nk pigeons, contradiction.

EXAMPLE

For example, suppose that 64 pigeons are placed in 7 pigeonholes. Show that some pigeonhole contains at least 10 pigeons.

If, otherwise, all pigeonholes had at most 9 pigeons, we would have at most 7x9=63 pigeons, contradiction.

Finally, let us remember the principle of mathematical induction.

- **Strong mathematical induction**

Remember the principle of mathematical induction for a statement P(n) which depends on the positive integer n. The steps are as follows

- **For n=1 the statement is true;**
- **Assume that the statement is true for n=k;**
- **Prove that the statement is true for n=k+1;**

Then the statement is true for any positive integer n.

But sometimes the inductive step is not based on the preceding integer but on all the preceding integers!

- **For n=1 the statement is true;**
- **Assume that the statement is true for any n<k;**
- **Prove that the statement is true for n=k;**

Then the statement is true for any positive integer n.

Although prime numbers will be formally introduced later on we will use a classical example which refers to prime numbers

Any integer $n\geq 2$ is either a prime or it has a prime divisor.

Proof by strong induction.

- For n=2 the statement is true since 2 is a prime.
- Assume that the statement is true for any n<k
- We will prove that it is true for n=k.

  Indeed, if k is a prime we are done. If not then k=ab
  But a<k hence it has a prime divisor p by assumption.
  Thus p divides k as well, i.e. p is a prime divisor of k

By strong induction the proposition is true for any $n\geq 2$.

2. DIVISIBILITY

For two integers a and b, we say that **a divides b,** if

$$b = ka \text{ for some } k \in Z$$

We use the notation $a \mid b$. **Thus**

$a \mid b$ **if and only if** $b = ka$ for some $k \in Z$

For example, 3 divides 15:

$3 \mid 15$ since $15 = 3 \times 5$

$3 \nmid 13$

We also say that

a is a **divisor** of b	e.g. 3 is a **divisor** of 15
a is a **factor** of b	e.g. 3 is a **factor** of 15
b is a **multiple** of a	e.g. 15 is a **multiple** of 3

Remark: Particularly for 0 and a non-zero integer a

$0 \mid 0$	(since 0 is a multiple of 0)
$a \mid 0$	(0 is a multiple of any integer, since $0 = 0a$)
$0 \nmid a$	(in other words, 0 divides only 0)

- ***Basic Properties***

1. $a \mid a$ for any $a \in Z$ (reflexive)
2. $a \mid b$ and $b \mid c \Rightarrow a \mid c$ (transitive)
3. $\pm 1 \mid a$ for any $a \in Z$
4. $a \mid \pm 1 \Rightarrow a = \pm 1$
5. $a \mid b$ and $b \mid a \Rightarrow a = \pm b$

Notice. We very often consider only positive integers. Then, the last three properties become

- $1 \mid a$ for any $a \in Z^+$
- $a \mid 1 \Rightarrow a=1$
- $a \mid b$ and $b \mid a \Rightarrow a=b$

The proofs of these properties are all similar. Let's see a proof.

Proof of property 2: $a \mid b$ and $b \mid c \Rightarrow a \mid c$

$a \mid b$ and $b \mid c \Rightarrow b=ka$ and $c=k'b$ for some $k, k' \in Z$ [by definition]

$\Rightarrow c=k'ka$

$\Rightarrow a \mid c$ [by definition]

Moreover, for any integers

6. $a \mid b \Rightarrow na \mid nb$
7. $na \mid nb$ and $n \neq 0 \Rightarrow a \mid b$ (cancellation)
8. $a_1 \mid b_1$ and $a_2 \mid b_2 \Rightarrow a_1 a_2 \mid b_1 b_2$
9. $a \mid b_1$ and $a \mid b_2 \Rightarrow \begin{cases} a \mid b_1+b_2 \\ a \mid b_1-b_2 \\ a \mid mb_1+nb_2 \quad \text{(any linear combination)} \end{cases}$

Proof of property 7: $na \mid nb$ and $n \neq 0 \Rightarrow a \mid b$

$na \mid nb$ and $n \neq 0 \Rightarrow nb=kna$ for some $k \in Z$ [by definition]

$\Rightarrow b=ka$ [since $n \neq 0$]

$\Rightarrow a \mid b$ [by definition]

- **Division of integers**

When we divide 41 by 5 (41÷5), the quotient is 8 and the remainder 1. More formally

$$41 = 5 \times 8 + 1$$

We also know that the remainder 1 satisfies $0 \le 1 < 5$. Thus

> Given two integers a and b>0, there exist q, r ∈Z such that
>
> $$a = bq + r \quad \text{with} \quad 0 \le r < b$$
>
> We say that q is the **quotient** and r is the **remainder**.

Mind the case where a is negative:

- When we divide 41 by 5 the remainder is 1 (see above).
- When we divide -41 by 5 the remainder is 4, since

$$-41 = 5 \times (-9) + 4$$

Finally, if r = 0 then b divides a since $a = bq$. For example, 40÷5 gives $40 = 5 \times 8$ and the remainder is 0.

NOTICE.

In fact, we can divide by negative integer b as well. But then

$$0 \le r < |b|$$

To summarize

- When we divide 41 by 5 or -5 the remainder is 1
- When we divide -41 by 5 or -5 the remainder is 4

Indeed,

$41 \div 5$	$41 = 5 \times 8 + 1$
$41 \div (-5)$	$41 = (-5) \times (-8) + 1$
$(-41) \div 5$	$-41 = 5 \times (-9) + 4$
$(-41) \div (-5)$	$-41 = -5 \times 9 + 4$

- **GCD and LCM**

The **greatest common divisor (gcd)** of two integers is just the greatest common divisor! ☺.

But bear in mind that it is always a non-negative number.

For example,

The gcd of 6 and 15 is 3. The gcd of 6 and -15 is still 3.

We write

$$gcd(6,15)=3 \quad \text{and} \quad gcd(6,-15)=3$$

But what is the formal definition of the gcd?

Let $a,b\in Z$. Then

$$gcd(a,b)=d \quad (d\geq 0)$$

if

(i) $d|a$ and $d|b$ [I.e. d is a common divisor]

(ii) If $d'|a$ and $d'|b$, then $d'|d$ [I.e. it is the greatest!]

Indeed, gcd(6,15)=3 since

(i) $3|6$ and $3|15$

(ii) if $d'|6$ and $d'|15$, then $d'|3$ [as d' can be either 1 or 3]

It also holds

$$gcd(0,a) = |a| \quad \text{and} \quad gcd(0,0) = 0$$

Proposition

For any $a,b\in Z$ it holds

(i) $gcd(a,b)=gcd(a+b,b)$

(ii) $gcd(a,b)=gcd(a-b,b)$

(iii) $gcd(a,b)=gcd(a+kb,b)$

We only prove property (iii) which is the most general result!

Proof of (iii)

Let $d_1=gcd(a,b)$ and $d_2=gcd(a+kb,b)$

$d_1|a$ and $d_1|b$ [property of d_1]

$\Rightarrow d_1|a+kb$ and $d_1|b$ [property of divisibility]

$\Rightarrow \mathbf{d_1 \leq d_2}$ [since $d_2=gcd(a+kb,b)$]

On the other hand

$d_2|\ a+kb$ and $d_2|a$ [property of d_1]

$\Rightarrow d_2|a+kb-kb$ and $d_2|b$ [property of divisibility]

$\Rightarrow d_2|a$ and $d_2|b$

$\Rightarrow \mathbf{d_2 \leq d_1}$ [since $d_1=gcd(a,b)$]

Therefore, $\mathbf{d_1=d_2}$

Similarly, the **least common multiple (lcm)** of two integers is just the least common non-negative multiple! ☺.

For example,

The lcm of 6 and 9 is 18.

We write

$$lcm(6,9)=18$$

But what is the formal definition of the lcm?

Let $a,b\in Z$. Then

$lcm(a,b)=\ell$ $(\ell \geq 0)$

if

(i) $a|\ell$ and $b|\ell$ [I.e. ℓ is a common multiple]

(ii) if $a|\ell'$ and $b|\ell'$, then $\ell|\ell'$ [I.e. it is the least]

Indeed, lcm(6,9)=18 since

(i) $6|18$ and $9|18$

(ii) if $6|\ell'$ and $9|\ell'$, then $18|\ell'$ [as ℓ' can be 18,36,54,72,...]

- **Euclidean Algorithm**

Our target here is to find gcd(a,b). If

$$a = bq + r$$

then according to a proposition above

$$gcd(a,b)=gcd(a-bq,b)=gcd(b,r)$$

Then we divide b by r

$$b = rq_1 + r_1$$

so that $gcd(b,r)= gcd(r,r_1)$ and so on!

Thus, we can find the gcd of two integers by repeated divisions.

Let's demonstrate the result by using an example:

Find gcd(100,18).

$$100 = \mathbf{18}\times 5 + \mathbf{10}$$
$$18 = \mathbf{10}\times 1 + \mathbf{8}$$
$$10 = \mathbf{8}\times 1 + \mathbf{2}$$
$$8 = \mathbf{2}\times 4 + \mathbf{0}$$

This implies that

$$gcd(100,18) = 2$$

Indeed,

$$gcd(100,18) = gcd(18,10) = gcd(10,8) = gcd(8,2) = gcd(2,0) = 2$$

This algorithm allows us also to 2= gcd(100,18) as a linear combination of 100 and 18:

$$\begin{aligned} 2 &= \mathbf{10}-1\times\mathbf{8} \\ &= \mathbf{10}-1\times(\mathbf{18}-1\times\mathbf{10}) = -1\times\mathbf{18}+2\times\mathbf{10} \\ &= -1\times\mathbf{18}+2\times(\mathbf{100}-5\times\mathbf{18}) = 2\times\mathbf{100}-11\times\mathbf{18} \end{aligned}$$

In general,

> For any $a,b\in Z$, if $gcd(a,b)=d$, then
>
> $d = sa+rb$ for some $r,s \in Z$

We say that the integers a and b are **coprime** if gcd(a,b)=1. For example 5 and 7 are coprime, 4 and 9 are coprime.

According to the last result, if a and b are coprime then

$$sa+rb = 1 \qquad \text{for some } r,s \in Z$$

But in this case the converse is also true, that is

$$\text{if } sa+rb = 1 \text{ for some } r,s \in Z, \text{ then } gcd(a,b)=1$$

Indeed, suppose that sa+rb = 1 and gcd(a,b)=d. Then

$$d|a \text{ and } d|b \Rightarrow d|sa+rb$$
$$\Rightarrow d|1$$
$$\Rightarrow d=1.$$

Therefore, we obtain a very strong result

$$gcd(a,b)=1 \iff sa+rb =1 \text{ for some } r,s \in Z$$

Based on this result we can prove the following

1. If gcd(a,b)=d then $\frac{a}{d}$ and $\frac{b}{d}$ are coprime integers.
2. If a|bc and a,b are coprime then a|c

Proofs

- $gcd(a,b)=d \Rightarrow sa+rb =d$ for some $r,s \in Z$

  $\Rightarrow s\frac{a}{d}+r\frac{b}{d} =1$ for some $r,s \in Z$ (clearly $\frac{a}{d},\frac{b}{d}$ integers)

  $\Rightarrow \frac{a}{d}$ and $\frac{b}{d}$ are coprime.

- Suppose that a|bc, and a,b are coprime. Then

  $sa+rb =1$ for some $r,s \in Z \Rightarrow sac+rbc =c$

  Since a|sac and a| rbc, it holds a|c.

3. PRIME NUMBERS

In this section we only consider positive integers.

Any number has at least two trivial divisors: 1 and itself. Some positive integers have only those two divisors. They are called **prime**. We consider that the smallest prime number is 2. This is in fact the only even prime number (why?)

A more formal definition says that an integer $p \geq 2$ is **prime** if

$$p=ab \Rightarrow a=1 \text{ or } b=1$$

The first prime numbers are

$$2, 3, 5, 7, 11, 13, 17, 23, \ldots$$

They form a sequence

$$p_n = \text{the } n\text{-th prime}$$

For example, $p_1=2$, $p_5=11$ etc.

Non-prime integers $n \geq 2$ are also called **composite**. 1 is neither prime nor composite. But how many prime numbers are there?

There are infinitely many prime numbers

Proof.

Suppose that there are only n prime numbers, $p_1, p_2, \ldots, p_n$.

Consider the integer

$$S= p_1p_2\ldots p_n+1$$

S has a prime divisor. Suppose it is p_i, where $1 \leq i \leq n$. Then

$$p_i \mid S \text{ and } p_i \mid p_1p_2\ldots p_n \Rightarrow p_i \mid (S-p_1p_2\ldots p_n)$$
$$\Rightarrow p_i \mid 1$$

Contradiction.

An interesting question is

Can we find 100 consecutive integers which are no prime?

The answer is YES. The numbers

$$101!+2,\quad 101!+3,\quad 101!+4,\quad \ldots,\quad 101!+101,$$

are 100 consecutive integers. The first one is divisible by 2, the second one by 3,…, the last one by 101. So, none of them is prime.

In general, the n consecutive integers

$$(n+1)!+2,\quad (n+1)!+3,\quad 101!+4,\quad \ldots,\quad (n+1)!+(n+1)$$

are composite numbers (why?)

- **Fundamental Theorem of Arithmetic**

We have already seen that

Any integer $n\geq 2$ has a prime divisor.

The proof has been done by using strong mathematical induction.

For example 60 is divisible by 2, but also by 3 etc. In fact we can express 60 as a product of primes:

$$60=2\times 2\times 3\times 5$$

We say that this is a **prime decomposition** of 60.

A stronger version of the last proposition says that any integer has a unique prime decomposition. This is the so-called fundamental theorem of Arithmetic. We split the proposition in two parts: Existence and Uniqueness.

Any integer $n\geq 2$ has a prime decomposition

Proof by strong induction.

- For n=2 it is true since 2 is already a prime.
- Assume that the statement is true for any n<k
- We will prove that it is true for n=k.
  Indeed, if k is a prime we are done. If not then k=ab
  But a<k and b<k, hence both a and b have prime decompositions. Thus k=ab also has a prime decomposition.

By strong induction the proposition is true for any n≥2.

But is it possible to express an integer into two different prime decompositions? The answer is NO.

Any integer n has a **unique** prime decomposition

Proof by strong induction.

- For n=2 it is true since 2 is the only prime decomposition for 2.
- Assume that the statement is true for any n<k
- We will prove that it is true for n=k.
  Indeed, if k is prime we are done. If not, suppose that

  $$k=p_1p_2\dots p_s=q_1q_2\dots q_t \quad \text{(where all } p_i \text{ and } q_i \text{ are prime)}$$

  Since p_1 divides the first product it also divides the second product. So it divides one of the primes q_i so it is one of them. Suppose (wlog) that $p_1=q_1$. Then

  $$p_2\dots p_s=q_2\dots q_t$$

  But this number is less that k so it has a unique decomposition. Therefore, s=t and

  $$p_2=q_2 \quad p_3=q_3 \quad \dots \quad p_s=q_s$$

  Thus the decomposition of k is unique.

By strong induction the proposition is true for any n≥2.

We agree that 1 has also a prime decomposition. It is a product of zero primes! Thus any positive integer has a prime decomposition.

NOTICE

There are three versions for the expression of the prime decomposition of a natural number n.

- $n = p_1 p_2 p_3 \cdots p_s$, where p_i primes with $p_1 \le p_2 \le \ldots \le p_s$
- $n = p_1^{n_1} p_2^{n_2} p_3^{n_3} \cdots p_s^{n_s}$, where p_i primes with $p_1 < p_2 < \ldots < p_s$
- $n = p_1^{n_1} p_2^{n_2} p_3^{n_3} \cdots$, where p_n is the sequence of all primes and only a finite number of exponents are non-zero

For example, the corresponding expressions for the natural number n=1400 are as follows

- $1400 = 2 \cdot 2 \cdot 2 \cdot 5 \cdot 5 \cdot 7$
- $1400 = 2^3 \cdot 5^2 \cdot 7$,
- $1400 = 2^3 3^0 5^2 7^1 11^0 13^0 \cdots$,

The prime decomposition also helps us to find the gcd and the lcm of two integers.

For example, since

$$1400 = 2^3 \cdot 5^2 \cdot 7,$$
$$151250 = 2 \cdot 5^4 \cdot 11^2,$$

we obtain

$$gcd(1400,151250) = 2 \cdot 5^2 = 50$$
$$lcm(1400,151250) = 2^3 \cdot 5^4 \cdot 7 \cdot 11^2 = 4235000$$

Clearly,

	the decomposition contains
gcd	only the common prime factors to the lowest power
lcm	all the prime factors to the greatest power.

This observation provides an easy proof for the following result

$$gcd(n,m) \times lcm(n,m) = nm$$

Indeed, if

$$n = p_1^{n_1} p_2^{n_2} p_3^{n_3} \cdots$$

$$m = p_1^{m_1} p_2^{m_2} p_3^{m_3} \cdots$$

(where p_n is the sequence of all primes), then

$$gcd(n,m) \times lcm(n,m) =$$

$$= (p_1^{\min(n_1,m_1)} p_2^{\min(n_2,m_2)} \cdots)(p_1^{\min(n_1,m_1)} p_2^{\min(n_2,m_2)} \cdots)$$

$$= p_1^{\min(n_1,m_1)+\max(n_1,m_1)} p_2^{\min(n_2,m_2)+\max(n_2,m_2)} \cdots$$

$$= p_1^{n_1+m_1} p_2^{n_2+m_2} \cdots$$

$$= (p_1^{n_1} p_2^{n_2} \cdots)(p_1^{m_1} p_2^{m_2} \cdots)$$

$$= nm$$

Let's confirm the result be using the example above:

$$1400 \times 151250 = 211750000$$

$$gcd \times lcm = 50 \times 4235000 = 211750000$$

4. LINEAR DIOPHANTINE EQUATIONS: ax+by=c

Equations where the solutions we are looking for are only integers are called **Diophantine**.

Here we study linear Diophantine equations of the form

$$ax+by=c$$

where the unknowns $x,y\in Z$.

Sometimes it is easy to see that there is no solution. For example

$$2x+6y=17$$

has no solution since the LHS is always even while the RHS is odd.

Consider now

$$2x+7y=9$$

Obviously (1,1) is a solution. But it is not the only one!

$$(1+7t,1-2t)$$

where $t\in Z$, are also solutions. Indeed

$$2(1+7t)+7(1-2t) = 2+14t+7-14t = 9$$

Thus (8,-1), (15,-3), (-6,3) are some of the many solutions.

In general, the following result holds.

Consider the linear Diophantine equation

$$ax+by=c$$

with $d=gcd(a,b)$.

- The equation has a solution **if and only if** $d|c$.
- Let (x_o,y_o) be a particular solution.
  (a) If $d=1$ the general solution is
  $$(x,y)=(x_o+bt,y_o-at)\,,\ t\in Z.$$
  (b) If $d\neq 1$ we divide the equation by d and reduce it to case (a) [thus $(x,y)=(x_o+\frac{b}{d}t,y_o-\frac{a}{d}t)\,,\ t\in Z$]

Proof.

Consider the equation

$$ax+by=c$$

If d does not divide c then it divides the LHS but not the RHS, contradiction.

If d divides c then

$$d=ra+sb \text{ for some } r,s\in Z \Rightarrow \frac{ra}{d}+\frac{sb}{d}=1$$
$$\Rightarrow \frac{rac}{d}+\frac{sbc}{d}=c$$
$$\Rightarrow a(r\frac{c}{d})+b(s\frac{c}{d})=c$$

Since $\frac{c}{d}\in Z$ the equation has a solution $(x_o,y_o)=(r\frac{c}{d}, s\frac{c}{d})$.

Let (x,y) be another solution. Then

$$ax+by=c$$
$$ax_o+by_o=c$$

Thus

$$ax+by=ax_o+by_o \Rightarrow a(x-x_o)=-b(y-y_o)$$
$$\Rightarrow \frac{-a}{b}=\frac{y-y_o}{x-x_o}$$

If d=1, that is a and b are coprime, then

$$y-y_o=-at$$
$$x-x_o=bt \qquad \text{for some } t\in Z$$

Therefore

$$(x,y)=(x_o+bt,y_o-at),\ t\in Z.$$

If $d\neq 1$ then

$$\frac{a}{d}x+\frac{b}{d}y=\frac{c}{d}$$

But now $gcd(\frac{a}{d},\frac{b}{d})=1$ and the general solution takes the form

$$(x,y)=(x_o+\frac{b}{d}t,y_o-\frac{a}{d}t),\ t\in Z.$$

EXAMPLE

Solve the Diophantine equations

(a) $6x+14y=21$ (b) $6x+13y=21$ (c) $6x+15y=21$

Solutions

(a) $\gcd(6,14)=2$. Since 2 does not divide 21, there is no solution.

(b) $\gcd(6,13)=1$. Since $1 \mid 21$, there is a solution.

The Euclidean algorithm gives

$$13=2\times6+1$$

Hence $1=13-6\times2$, that is $6\times(-2)+13\times1=1$

Multiply by 21: $6\times(-42)+13\times21=21$

A particular solution is $(-42,21)$

The general solution is $(-42+13t,21-6t)$

(c) $\gcd(6,15)=3$. Since $3 \mid 21$, there is a solution.

Method A: Direct

The Euclidean algorithm gives

$$15=2\times6+3$$

$$6 = 2\times3+0 \quad \text{(thus gcd=3)}$$

Hence $3=15-6\times2$, that is $6\times(-2)+15\times1=3$

Multiply by 7: $6\times(-14)+13\times7=21$

A particular solution is $(-14,7)$

The general solution is $(-14+5t,7-2t)$

Method B: divide the equation by 3; it reduces to case gcd=1

$$2x+5y=7$$

Now $\gcd(2,5)=1$.

The Euclidean algorithm gives

$$5 = 2\times2+1$$

Hence $1=5-2\times2$, that is $2\times(-2)+5\times1=1$

Multiply by 7: $2\times(-14)+5\times7=7$

A particular solution is $(-14,7)$

The general solution is $(-14+5t,7-2t)$

5. CONGRUENCES

For any $n \in Z^+$, we define the equivalence relation in Z

$$a \equiv b \pmod{n} \Leftrightarrow n \mid a-b$$

or equivalently

$\Leftrightarrow$ a and b leave the same remainder when divided by n

We say that a and b are **congruent modulo n** (and the equivalence relation is called **congruence**).

For example

$$27 \equiv 12 \pmod{5}$$

There are 5 equivalence classes modulo 5,

$0 \pmod 5$ it is the set $\{5k \mid k \in Z\}$
$1 \pmod 5$ it is the set $\{5k+1 \mid k \in Z\}$
$2 \pmod 5$ it is the set $\{5k+2 \mid k \in Z\}$
$3 \pmod 5$ it is the set $\{5k+3 \mid k \in Z\}$
$4 \pmod 5$ it is the set $\{5k+4 \mid k \in Z\}$

In general, there are n equivalence classes modulo n

$0 \pmod n$
$1 \pmod n$
$2 \pmod n$
...
$(n-1) \pmod n$

They are also known as **residue classes** modulo n.

The question "find $27 \pmod 5$" means find the corresponding residue class. Thus

$$27 \equiv 2 \pmod{5}$$

As the congruence modulo n reduces to divisibility, some first results are trivial

- **Properties of congruences**

Let

$$a\equiv b(\mathrm{mod}n) \quad \text{and} \quad c\equiv d(\mathrm{mod}n)$$

Then

- $a+c\equiv b+d(\mathrm{mod}n)$
- $a-c\equiv b-d(\mathrm{mod}n)$
- $ac\equiv bd(\mathrm{mod}n)$

Proofs.

$$a\equiv b(\mathrm{mod}n) \Rightarrow n \mid a-b$$
$$c\equiv d(\mathrm{mod}n) \Rightarrow n \mid c-d$$

1st property: just notice that

$$n \mid (a-b)+(c-d) = (a+c)-(b+d)$$
$$\Rightarrow a+c\equiv b+d(\mathrm{mod}n)$$

2nd property: similarly

3rd property:

$$n \mid (a-b)(c-d) = ac-bc-ad+bd$$
$$= ac-bc-ad+2bd-bd$$
$$= ac-bd-(bc-bd)-(ad-bd)$$
$$= ac-bd-b(c-d)-d(a-b)$$

Hence

$$n \mid ac-bd$$
$$\Rightarrow ac\equiv bd(\mathrm{mod}n)$$

Based on these properties we can also prove the following

Let $a\equiv b(\mathrm{mod}n)$

Then

- $a^k\equiv b^k(\mathrm{mod}n)$ $k\in Z^+$
- $ma\equiv mb(\mathrm{mod}n)$ $m\in Z$
- $f(a)\equiv f(b)(\mathrm{mod}n)$ where f is a polynomial with integer coefficients

- **Fermat's Little theorem**

> For any $a \in Z$ and prime p that does not divide a,
> $a^{p-1} \equiv 1 (\mod p)$

For example

$$3^4 \equiv 1 (\mod 5)$$
$$5^{12} \equiv 1 (\mod 13)$$

This theorem helps us to find the residue class of a large number.

EXAMPLE

Find $5^{2018} (\mod 13)$

Solution

By Fermat's little theorem

$$5^{12} \equiv 1 (\mod 13) \Rightarrow 5^{12 \times 168} \equiv 1^{168} (\mod 13)$$
$$\Rightarrow 5^{2016} \equiv 1 (\mod 13)$$
$$\Rightarrow 5^{2016} 5^2 \equiv 5^2 (\mod 13)$$
$$\Rightarrow 5^{2018} \equiv 25 (\mod 13)$$
$$\Rightarrow 5^{2018} \equiv 12 (\mod 13)$$

Sometimes we cannot start by using Fermat, but we try to start by a similar relation of the form $a^n \equiv 1 (\mod n)$ or $a^n \equiv -1 (\mod n)$.

EXAMPLE

Find the last digit of 3^{2018}. In other words, find $3^{2018} (\mod 10)$

Solution

Method 1: We observe that $3^4 \equiv 1 (\mod 10)$.

Thus
$$3^{4 \times 504} \equiv 1^{504} (\mod 10)$$
$$\Rightarrow 3^{2016} \equiv 1 (\mod 10)$$
$$\Rightarrow 3^{2016} 3^2 \equiv 3^2 (\mod 10)$$
$$\Rightarrow 3^{2018} \equiv 9 (\mod 10)$$

Thus the last digit is 9.

Method 2: We observe that $3^2 \equiv -1 (mod10)$.

Thus $3^{2\times1009} \equiv (-1)^{1009} (mod10)$

$\Rightarrow 3^{2018} \equiv -1 (mod10)$

$\Rightarrow 3^{2018} \equiv 9 (mod10)$

Thus the last digit is 9.

NOTICE

- It is not always possible to start with a relation of the form
  $a^n \equiv 1 (modn)$ or $a^n \equiv -1 (modn)$.
  We must improvise by using similar techniques.
- For $x^n (modn)$ with $x>n$ we can simplify the base x by choosing a congruent base y modulo n (since $x \equiv y (modn) \Rightarrow x^n \equiv y^n (modn)$.

EXAMPLE

Find the last digit of 2018^{2018}, that is $2018^{2018} (mod10)$

Solution

Firstly, we reduce the base 2018 to a smaller one:

$$2018 \equiv -2 (mod10) \Rightarrow 2018^{2018} \equiv (-2)^{2018} (mod10)$$
$$\Rightarrow 2018^{2018} \equiv 2^{2018} (mod10)$$

Thus the problem reduces to finding $2^{2018} (mod10)$.

[2^n is always even, thus we can't start by $2^n \equiv 1 (mod10)$ for some n. There are many alternative methods; I suggest one]

We observe that $2^4 \equiv 1 (mod5)$.

Thus $2^{4\times504} \equiv 1^{504} (mod5) \Rightarrow 2^{2016} \equiv 1 (mod5)$

$\Rightarrow 2^{2017} \equiv 2 (mod5)$

But also $2^{2017} \equiv 2 (mod2)$.

Thus $2^{2017} \equiv 2 (mod2\times5) \Rightarrow 2^{2017} \equiv 2 (mod10)$

$\Rightarrow 2\times2^{2017} \equiv 2\times2 (mod10)$

$\Rightarrow 2^{2018} \equiv 4 (mod10)$

Therefore, the last digit of 2018^{2018} is 4.

- **Solving linear congruences**

Consider the linear congruence equation

$$3x \equiv 4 (\mathrm{mod}\, 5)$$

Notice that if x=a satisfies the equation then the whole class

$$a (\mathrm{mod}\, 5)$$

satisfies the equation (easy to verify).

Among the 5 classes mod5 only 3(mod5) satisfies the equation since

$$3 \times 3 = 9 \equiv 4 (\mathrm{mod}\, 5)$$

In general,

Consider the linear congruence

$$ax \equiv b (\mathrm{mod}\, n)$$

with $d=\gcd(a,n)$.

- The equation has a solution **if and only if** $d \mid b$.

  (a) If $d=1$ there is a unique solution of the form

  $$x_o (\mathrm{mod}\, n)$$

  (b) If $d \neq 1$ we divide the whole equation by d and get

  $$a'x \equiv b' (\mathrm{mod}\, n')$$

  It reduces to case (a).

  Given the unique solution $x_o (\mathrm{mod}\, n')$, we obtain d solutions modn:

  x_o, $x_o + n'$, $x_o + 2n'$, …, $x_o + (d-1)n'$ all (modn)

In fact the problem of solving a linear congruent is equivalent to the problem of solving a Diophantine equation. Indeed,

$$ax \equiv b (\mathrm{mod}\, n) \Leftrightarrow ax - b = nk$$
$$\Leftrightarrow ax - nk = b$$

In Diophantine equations we seek pairs (x,k),

In linear congruences we seek classes x(modn) [ignore k]

Thus the strategies are very similar.

We saw in a previous paragraph an example of 3 Diophantine equations

(a) $6x+14y=21$ (b) $6x+13y=21$ (c) $6x+15y=21$

Let us see now the 3 corresponding linear congruences.

EXAMPLE

Solve the linear congruences

(a) $6x\equiv 21 \pmod{14}$

(b) $6x\equiv 21 \pmod{13}$

(c) $6x\equiv 21 \pmod{15}$

Solutions

(a) $\gcd(6,14)=2$.

Since 2 does not divide 21, there is **no solution**.

(b) $\gcd(6,13)=1$.

Since $1 \mid 21$, there is **a unique solution mod13**.

The Euclidean algorithm gives

$$13=2\times 6+1$$

Hence $1=13-6\times 2$, that is $6\times(-2)+13\times 1=1$

Multiply by 21: $6\times(-42)+13\times 21=21$

The solution is $-42 \pmod{13}$, that is **$10 \pmod{13}$**

(c) $\gcd(6,15)=3$.

Since $3 \mid 21$, there are **3 solutions (mod15)**.

Divide the equation by 3:

$$2x\equiv 7 \pmod 5$$

Now $\gcd(2,5)=1$. The Euclidean algorithm gives

$$5 = 2\times 2+1$$

Hence $1=5-2\times 2$, that is $2\times(-2)+5\times 1=1$

Multiply by 7: $2\times(-14)+5\times 7=7$

The solution is $-14 \pmod 5$, that is $1 \pmod 5$

The 3 solutions (mod15) are the following

$1 \pmod{15}$ **$6 \pmod{15}$** **$11 \pmod{15}$**

- **Chinese Remainder Theorem**

> Consider the simultaneous linear congruences
>
> $$x\equiv b_1(\mathrm{mod}n_1)$$
> $$x\equiv b_2(\mathrm{mod}n_2)$$
> $$\dots$$
> $$x\equiv b_k(\mathrm{mod}n_k)$$
>
> If $n_1, n_2,\dots, n_k$ are pairwise coprime and $n=n_1n_2\dots n_k$ there is a unique solution mod$n$.

Sketch of the proof for 3 congruences

$$x\equiv b_1(\mathrm{mod}n_1)$$
$$x\equiv b_2(\mathrm{mod}n_2)$$
$$x\equiv b_3(\mathrm{mod}n_3)$$

Existence

- we form 3 auxiliary linear congruences

  $n_2n_3A \equiv 1(\mathrm{mod}n_1)$

  $n_1n_3B \equiv 1(\mathrm{mod}n_2)$

  $n_1n_2C \equiv 1(\mathrm{mod}n_3)$
- we find the particular solutions A, B, C
- We calculate $x\equiv b_1(n_2n_3A)+b_2(n_1n_3B)+b_3(n_1n_2C)$

The integer x satisfies the 3 congruences (easy to check).

Uniqueness

If another integer y also satisfies the 3 equations then

$$x\equiv y(\mathrm{mod}n_1)$$
$$x\equiv y(\mathrm{mod}n_2)$$
$$x\equiv y(\mathrm{mod}n_3)$$

Thus n_1,n_2,n_3 divide $x-y$ and since they are pairwise coprime

$$n=n_1n_2n_3 \text{ divides } x-y$$

that is

$$x\equiv y(\mathrm{mod}n)$$

EXAMPLE

Solve the system of linear congruences

$$x\equiv 1(\mathrm{mod}2)$$
$$x\equiv 2(\mathrm{mod}3)$$
$$x\equiv 4(\mathrm{mod}5)$$

Solution

Since 2,3,5 are pairwise coprime there is a unique solution mod30.

Method 1 (it follows the rationale of the proof)

- we form 3 auxiliary linear congruences

$$3\times 5A\equiv 1(\mathrm{mod}2) \quad i.e \quad 15A\equiv 1(\mathrm{mod}2)$$
$$2\times 5B\equiv 1(\mathrm{mod}3) \quad i.e \quad 10B\equiv 1(\mathrm{mod}3)$$
$$2\times 3C\equiv 1(\mathrm{mod}5) \quad i.e \quad 6C\equiv 1(\mathrm{mod}5)$$

- we find the particular solutions A=1, B=1, C=1
- We estimate $x\equiv 1(15A)+2(10B)+4(6C) = 15+20+24 = 59$

The solution is $x\equiv 59(\mathrm{mod}30)$, that is **$x\equiv 29(\mathrm{mod}30)$.**

Method 2 (more practical)

1^{st} equation $\Rightarrow x= 2a+1$

2^{nd} equation $\Rightarrow 2a+1\equiv 2(\mathrm{mod}3) \Rightarrow 2a\equiv 1(\mathrm{mod}3) \Rightarrow a\equiv 2(\mathrm{mod}3)$

hence $a=3b+2 \Rightarrow x=2(3b+2)+1 \Rightarrow x=6b+5$

3^{rd} equation $\Rightarrow 6b+5\equiv 4(\mathrm{mod}5) \Rightarrow 6b\equiv -1(\mathrm{mod}5) \Rightarrow b=4$

Therefore $x = 29$ and the solution is **$x\equiv 29(\mathrm{mod}30)$.**

- **More general form of the Chinese Remainder Theorem**

$$a_1x\equiv c_1(\mathrm{mod}n_1)$$
$$a_2x\equiv c_2(\mathrm{mod}n_2)$$
$$a_3x\equiv c_3(\mathrm{mod}n_3)$$

We solve the 3 linear congruences separately.

Suppose they have unique solutions: $x\equiv b_1(\mathrm{mod}n_1)$

$$x\equiv b_2(\mathrm{mod}n_2)$$
$$x\equiv b_3(\mathrm{mod}n_3)$$

Thus the problem reduces to the simple case above.

If for example the first congruence has 2 solutions

$$x\equiv b_1(\mod n_1) \text{ and } x\equiv b_1'(\mod n_1)$$

(and the other two unique) we have to solve two distinct systems

$$\begin{array}{ll} x\equiv b_1(\mod n_1) & x\equiv b_1'(\mod n_1) \\ x\equiv b_2(\mod n_2) & x\equiv b_2(\mod n_2) \\ x\equiv b_3(\mod n_3) & x\equiv b_3(\mod n_3) \end{array}$$

EXAMPLE

Solve the system of linear congruences

$$3x\equiv 1(\mod 2)$$
$$5x\equiv 1(\mod 3)$$
$$2x\equiv 3(\mod 5)$$

Solution

$3x\equiv 1(\mod 2)$ has the unique solution $x\equiv 1(\mod 2)$

$5x\equiv 1(\mod 3)$ has the unique solution $x\equiv 2(\mod 3)$

$2x\equiv 3(\mod 5)$ has the unique solution $x\equiv 4(\mod 5)$

The three new congruences form in fact the system of the previous example, so the solution is $\mathbf{x\equiv 29(\mod 30)}$.

EXAMPLE

Solve the system of linear congruences

$$2x\equiv 1(\mod 3)$$
$$6x\equiv 2(\mod 4)$$

Solution

The 1st equation has the unique solution $x\equiv 2(\mod 3)$.

The 2nd equation has the two solutions $x\equiv 1(\mod 4)$ and $x\equiv 3(\mod 4)$.

We obtain two systems

$$\begin{array}{ll} x\equiv 2(\mod 3) & x\equiv 2(\mod 3) \\ x\equiv 1(\mod 4) & x\equiv 3(\mod 4) \end{array}$$

The first system has the solution $\mathbf{x\equiv 5(\mod 12)}$.

The second system has the solution $\mathbf{x\equiv 11(\mod 12)}$.

An interesting application of the Chinese remainder theorem is given below. It provides an additional tool for finding the residue class of a large number.

EXAMPLE

Find $7^{2018}(\text{mod}30)$ by using Chinese remainder theorem.

Solution

Since $30=2\times3\times5$, we split the question into 3 problems:

Problem 1: Find $7^{2018}(\text{mod}2)$

$7\equiv1(\text{mod}2) \Rightarrow 7^{2018}\equiv1(\text{mod}2)$

Problem 2: Find $7^{2018}(\text{mod}3)$

$7\equiv1(\text{mod}3) \Rightarrow 7^{2018}\equiv1(\text{mod}3)$

Problem 3: Find $7^{2018}(\text{mod}5)$

$7\equiv2(\text{mod}5) \Rightarrow 7^{2018}\equiv2^{2018}(\text{mod}5)$

Thus we have to find $2^{2018}(\text{mod}5)$

$2^4\equiv1(\text{mod}5) \Rightarrow 2^{4\times504}\equiv1^{504}(\text{mod}5)$

$\Rightarrow 2^{2016}\equiv1(\text{mod}5)$

$\Rightarrow 2^{2018}\equiv2^2(\text{mod}5)$

$\Rightarrow 7^{2018}\equiv4(\text{mod}5)$

Thus $x=7^{2018}$ satisfies the equations

$$x\equiv1(\text{mod}2)$$
$$x\equiv1(\text{mod}3)$$
$$x\equiv4(\text{mod}5)$$

By using the Chinese remainder theorem, there is a unique solution mod30:

1^{st} equation $\Rightarrow x= 2a+1$

2^{nd} equation $\Rightarrow 2a+1\equiv1(\text{mod}3) \Rightarrow 2a\equiv0(\text{mod}3) \Rightarrow a\equiv0(\text{mod}3)$

hence $a=3b \Rightarrow x=2(3b)+1 \Rightarrow x=6b+1$

3^{rd} equation $\Rightarrow 6b+1\equiv4(\text{mod}5) \Rightarrow 6b\equiv3(\text{mod}5) \Rightarrow b=3$

Therefore $x = 19$

The solution is $\mathbf{x\equiv19(\text{mod}30)}$.

---

6. REPRESENTATION OF NUMBERS

- **The decimal system vs the base-b system**

The standard system of expressing numbers is the **decimal system** (or **base-10 system**) which uses 10 digits

$$0, 1, 2, 3, 4, 5, 6, 7, 8, 9$$

An integer in this system has an expression of the form

$$a_n a_{n-1} \cdots a_2 a_1 a_0$$

which implies

$$a_0 + a_1 10 + a_2 10^2 + \cdots + a_{n-1} 10^{n-1} + a_n 10^n$$

Following the same rationale we can express an integer by using b digits in the **base-b system**

$$a_0 + a_1 b + a_2 b^2 + \cdots + a_{n-1} b^{n-1} + a_n b^n$$

For example, in the base 5 system we use only 5 digits

$$0,1,2,3,4$$

The number 24103 in the base-5 system is equal to

$$3 + 0 \times 5 + 1 \times 5^2 + 4 \times 5^3 + 2 \times 5^4$$

that is 1778 in the decimal system.

We write

$$(24103)_5 = (1778)_{10}$$

Thus, the process of translating a number to the decimal system

$$(24103)_5 = (?)_{10}$$

is straightforward (just performing the analysis above).

What about the inverse process? For example

$$(1778)_{10} = (?)_5$$

We divide continuously by 5:

1778 : 5	quotient 355,	remainder = 3
355 : 5	quotient 71,	remainder = 0
71 : 5	quotient 14,	remainder = 1
14 : 5	quotient 2,	remainder = 4
2 : 5	quotient 0,	remainder = 2

We just write the remainders in the opposite order

$$(1778)_{10} = (24103)_5$$

EXAMPLE

Express the number $(196)_{10}$ in the **binary** (i.e. **base-2**) system.

Solution

196 : 2	quotient 98,	remainder = 0
98 : 2	quotient 49,	remainder = 0
49 : 2	quotient 24,	remainder = 1
24 : 2	quotient 12,	remainder = 0
12 : 2	quotient 6,	remainder = 0
6 : 2	quotient 3,	remainder = 0
3 : 2	quotient 1,	remainder = 1
1 : 2	quotient 0,	remainder = 1

Thus

$$(196)_{10} = (11000100)_5$$

In the base-16 system we use the 16 digits

0, 1, 2, 3, 4, 5, 6, 7, 8, 9, A, B, C, D, E, F

EXAMPLE

Express $(2AF3)_{16}$

(a) In the decimal system

(b) In the binary system

Solution

(a) $$(2AF3)_{16} = 3 + F \times 16 + A \times 16^2 + 2 \times 16^3$$
$$= 3 + 15 \times 16 + 10 \times 16^2 + 2 \times 16^3$$
$$= (10995)_{10}$$

(b) **Method 1:** we can divide continuously 10995 (decimal) by 2.
We will find $(10101011110011)_2$

Method 2: (applies in the base-4, base-8, base-16 systems)
We translate each base-16 digit in binary form of length 4

$2 \to 0010$ $A \to 1010$ $F \to 1111$ $3 \to 0011$

Thus the binary form is $(\underline{\ \ 10}\ \underline{1010}\ \underline{1111}\ \underline{0011})_2$

- **Divisibility tests (in the decimal system)**

Consider the integer a in the decimal system

$$a = (a_n a_{n-1} \cdots a_1 a_0)_{10}$$
$$= a_n 10^n + a_{n-1} 10^{n-1} + \cdots + a_1 10 + a_0$$

We can test if a is divisible by 2,3,4,5,6,7,8,9,10 or 11 as follows

Division by 2

a is divisible by 2 ⇔ the last digit of a is even

Proof.

$$a = a_n 10^n + a_{n-1} 10^{n-1} + \cdots + a_1 10 + a_0$$
$$\equiv 0 + 0 + \cdots + 0 + a_0 \pmod 2$$
$$\equiv a_0 \pmod 2$$

Therefore

$$2 \mid a \Leftrightarrow 2 \mid a_0$$

For example,

37532268 is divisible by 2 since 8 (**last digit**) is even

Division by 3

a is divisible by 3 ⇔ the sum of the digits is divisible by 3

Proof.

We first observe that for any $k \in Z^+$

$$10 \equiv 1 \pmod 3 \Rightarrow 10^k \equiv 1 \pmod 3$$

Thus,

$$a = a_n 10^n + a_{n-1} 10^{n-1} + \cdots + a_1 10 + a_0$$
$$\equiv a_n + a_{n-1} + \cdots + a_1 + a_0 \pmod 3$$

Therefore

$$3 \mid a \Leftrightarrow 3 \mid \text{sum of digits}$$

For example,

37532268 is divisible by 3

since **sum of digits** = 36 which is divisible by 3

Division by 4

a is divisible by 4 ⇔ $(a_1a_0)_{10}$ (last 2 digits) is divisible by 4

Proof.

We first observe that $k\in Z^+$ with $k\geq 2$

$$10^k \equiv 0 (\mathrm{mod}4) \quad \text{(since 100, 1000 etc. are divisible by 4)}$$

Thus,

$$\begin{aligned} a &= a_n 10^n + a_{n-1}10^{n-1} + \cdots + a_1 10 + a_0 \\ &\equiv 10a_1 + a_0 \ (\mathrm{mod}4) \\ &\equiv (a_1a_0)_{10} \ (\mathrm{mod}4) \end{aligned}$$

Therefore

$$4 \mid a \Leftrightarrow 4 \mid (a_1a_0)_{10}$$

For example,

37532268 is divisible by 4

since 68 (**last 2 digits**) is divisible by 4

Division by 5

a is divisible by 5 ⇔ the last digit is either 0 or 5

Proof.

$$\begin{aligned} a &= a_n 10^n + a_{n-1}10^{n-1} + \cdots + a_1 10 + a_0 \\ &\equiv 0 + 0 + \cdots + 0 + a_0 \ (\mathrm{mod}5) \\ &\equiv a_0 \ (\mathrm{mod}5) \end{aligned}$$

Therefore

$$5 \mid a \Leftrightarrow 5 \mid a_0 \Leftrightarrow a_0 \text{ is 0 or 5}$$

For example,

37532268 is not divisible by 5 since the **last digit** is 8

Division by 6

a is divisible by 6 ⇔ it is divisible by 2 and by 3

For example,

37532268 is divisible by 6 since it is divisible **by 2** and **by 3**

Division by 7

a is divisible by 7 $\Leftrightarrow (a_n a_{n-1}\cdots a_1)_{10} - 2a_0$ is divisible by 7

Proof.

$$\begin{aligned} 2a &= 2(a_n 10^n + a_{n-1}10^{n-1} + \cdots + a_1 10 + a_0) \\ &= 2(a_n 10^n + a_{n-1}10^{n-1} + \cdots + a_1 10) + 2a_0 \\ &= 20(a_n 10^{n-1} + a_{n-1}10^{n-2} + \cdots + a_1) + 2a_0 \\ &\equiv -(a_n 10^{n-1} + a_{n-1}10^{n-1} + \cdots + a_1) + 2a_0 \pmod 7 \\ &\equiv -(a_n a_{n-1}\cdots a_1)_{10} + 2a_0 \bmod 7 \end{aligned}$$

Therefore

$$7 \mid a \;\Leftrightarrow\; 7 \mid 2a \;\Leftrightarrow\; 7 \mid (a_n a_{n-1}\cdots a_1)_{10} - 2a_0$$

For example, for **3753226**8 is not divisible by 7 since

check 3753226 - 2×8 = **3753210**
check 375321 - 2×0 = **375321**
check 37532 - 2×1 = **37530**
check 3753 - 2×0 = **3753**
check 375 - 2×3 = **369**
check 36 - 2×9 = 18 which is not divisible by 7

Division by 8

a is divisible by 8 $\Leftrightarrow (a_2 a_1 a_0)_{10}$ (last 3 digits) is divisible by 8

Proof.

We first observe that for any $k \in Z^+$ with $k \geq 3$

$10^k \equiv 0 \pmod 8$ (since 1000, 10000 etc. are divisible by 8)

Thus,

$$\begin{aligned} a &= a_n 10^n + a_{n-1}10^{n-1} + \cdots + a_1 10 + a_0 \\ &\equiv 100a_2 + 10a_1 + a_0 \pmod 8 \\ &\equiv (a_2 a_1 a_0)_{10} \pmod 8 \end{aligned}$$

Therefore $8 \mid a \Leftrightarrow 8 \mid (a_2 a_1 a_0)_{10}$

For example,

37532**268** is not divisible by 8

since 268 (**last 3 digits**) is not divisible by 8.

Division by 9

a is divisible by 9 ⇔ the sum of the digits is divisible by 9

Proof.

We first observe that for any $k \in Z^+$

$$10 \equiv 1 (mod 9) \Leftrightarrow 10^k \equiv 1 (mod 9)$$

Thus,

$$\begin{aligned} a &= a_n 10^n + a_{n-1} 10^{n-1} + \cdots + a_1 10 + a_0 \\ &\equiv a_n + a_{n-1} + \cdots + a_1 + a_0 \ (mod 9) \end{aligned}$$

Therefore

$$9 \mid a \Leftrightarrow 9 \mid \text{sum of digits}$$

For example,

37532268 is divisible by 9

since **sum of digits** = 36 which is divisible by 9

Division by 10

a is divided by 10 ⇔ the last digit is 0

Proof.

$$\begin{aligned} a &= a_n 10^n + a_{n-1} 10^{n-1} + \cdots + a_1 10 + a_0 \\ &\equiv 0 + 0 + \cdots + 0 + a_0 \ (mod 10) \\ &\equiv a_0 \ (mod 10) \end{aligned}$$

Therefore

$$\begin{aligned} 10 \mid a &\Leftrightarrow 10 \mid a_0 \\ &\Leftrightarrow a_0 \text{ is } 0 \end{aligned}$$

For example,

37532268 is not divisible by 10

since the last digit is not 0

Among the two-digit divisors the case of 11 is quite interesting.

Division by 11

a is divided by 11 ⇔ $a_0-a_1+a_2-a_3+\ldots$ is divisible by 11

Proof.

We first observe that for any $k\in Z^+$

$$10 \equiv -1(mod11) \Rightarrow 10^k \equiv 1(mod11) \quad \text{if k is even}$$
$$\Rightarrow 10^k \equiv -1(mod11) \quad \text{if k is odd}$$

Thus,

$$a = a_0 + a_1 10 + \cdots + a_{n-1}10^{n-1} + a_n 10^n$$
$$\equiv a_0 - a_1 + a_2 - a_3 + \cdots (mod11)$$

Therefore

$$11 \mid a \Leftrightarrow 11 \mid a_0 - a_1 + a_2 - a_3 + \cdots$$

For example,

37532268 is not divisible by 11

since 8-6+2-2+3-5+7-3 = 4 is not divisible by 11

while

737532268 is divisible by 11

since 8-6+2-2+3-5+7-3+7 = 11 is divisible by 11

Division by 12

a is divisible by 12 ⇔ it is divisible by 3 and by 4

For example,

37532268 is divisible by 12 since it is divisible **by 3** and **by 4**

We may obtain similar tests by combining existing cases. For example,

a is divisible by 15 ⇔ it is divisible by 3 and by 5

a is divisible by 33 ⇔ it is divisible by 3 and by 11

and so on.

7. RECURRENCE RELATIONS

Let us start with two familiar cases

- **Arithmetic sequences**

An arithmetic sequence of common difference d is defined by a recurrence relation

$$u_n = u_{n-1} + d,$$

with u_1 given

Then, the general term can be found directly by the formula

$$u_n = u_1 + (n-1)d$$

For example,

$$\text{if } u_1 = 10 \text{ and } u_n = u_{n-1} + 3,$$

then,

$$u_n = 10 + (n-1)3 = 3n + 7$$

Notice:

The general term is always a linear expression of n: $u_n = an + b$

- **Geometric sequences**

A geometric sequence of common ratio r is defined by a recurrence relation

$$u_n = r u_{n-1},$$

with u_1 given

Then, the general term can be found directly by the formula

$$u_n = u_1 r^{n-1}$$

For example,

$$\text{if } u_1 = 12 \text{ and } u_n = 3u_{n-1},$$

then,

$$u_n = 12 \times 3^{n-1} = 4 \times 3^n$$

Notice:

The general term is always an exponential expression of n: $u_n = ar^n$

- **Recurrence relations of first degree**

In a recurrence relation of first degree the term u_n of a sequence is given in terms of u_{n-1}. Here we study the linear case of such a relation:

$$u_n = ru_{n-1} + d$$

Notice:

if $r = 1$ we obtain an arithmetic sequence: $u_n = u_{n-1} + d$

if $d = 0$ we obtain a geometric sequence: $u_n = ru_{n-1}$

For more general cases the following proposition holds:

Let $u_n = ru_{n-1} + d, \quad (r \neq 1)$

[u_1 is given]

The general term has the form

$$u_n = ar^n + b$$

The values of the first two terms u_1, u_2 help us to find the parameters a and b.

EXAMPLE

Given that $u_1 = 5$ and $u_n = 3u_{n-1} + 7$ find a general term of u_n

Solution

The general solution has the form

$$u_n = a3^n + b$$

Since $u_1 = 5$, $3a + b = 5$

We find $u_2 = 22$, thus $9a + b = 22$

The simultaneous equations give $a = \frac{17}{6}$ and $b = -\frac{7}{2}$

Therefore,

$$u_n = \frac{17}{6}3^n - \frac{7}{2}$$

- **Recurrence relations of second degree (homogeneous case)**

In a recurrence relation of second degree the term u_n of a sequence is given in terms of u_{n-1} and u_{n-2}. There is no difference

if u_{n+1} is given in terms of u_n and u_{n-1}
or if u_{n+2} is given in terms of u_{n+1} and u_n.

Here we only study the so called "homogeneous case" where:

$$u_{n+2} + Au_{n+1} + Bu_n = 0 \quad (A,B \text{ constants})$$

Notice that, if a solution has the form $u_n = r^n$ then it holds

$$r^{n+2} + Ar^{n+1} + Br^n = 0$$

$$\Rightarrow r^2 + Ar + B = 0$$

The latter is known as the **characteristic** (or **auxiliary**) equation of the recurrence relation.

The following proposition provides the general solution of the problem.

Let $u_{n+2} + Au_{n+1} + Bu_n = 0$,
$[u_1, u_2$ are given$]$

We solve the **characteristic** (or **auxiliary**) equation

$$r^2 + Ar + B = 0$$

- In case of 2 distinct roots r_1, r_2 (either real or complex) the general solution has the form
$$u_n = ar_1^n + br_2^n$$
- In case of 1 double root r_1, the general solution has the form
$$u_n = ar_1^n + bnr_1^n$$

The values of the first two terms u_1, u_2 help us to find the parameters a and b.

EXAMPLE

Solve the recurrence relation problems

(a) $u_{n+2} - 4u_{n+1} + 3u_n = 0, \quad u_0 = 5,\ u_1 = 7$

(b) $u_{n+2} - 4u_{n+1} + 4u_n = 0, \quad u_0 = 5,\ u_1 = 8$

(c) $u_{n+2} - 4u_{n+1} + 5u_n = 0, \quad u_0 = 4,\ u_1 = 8$

Solution

(a) The characteristic equation is

$$r^2 - 4r + 3 = 0$$

The solutions are 1 and 3. Thus the general solution has the form

$$u_n = a1^n + b3^n = a + b3^n$$

The first two terms give

$$a + b = 5 \qquad \text{and} \qquad a + 3b = 7$$

Thus $a = 4, b = 1$ and the general solution is $u_n = 4 + 3^n$

(b) The characteristic equation is

$$r^2 - 4r + 4 = 0$$

The solution is 2. Thus the general solution has the form

$$u_n = a2^n + bn2^n$$

The first two terms give

$$a = 5 \qquad \text{and} \qquad 2a + 2b = 8$$

Thus $a = 5, b = -1$ and the general solution is $u_n = (5 - n)2^n$

(c) The characteristic equation is

$$r^2 - 4r + 5 = 0$$

The solutions are $2 \pm i$. Thus the general solution has the form

$$u_n = a(2 + i)^n + b(2 - i)^n$$

The first two terms give

$$a + b = 4$$

$$2a + 2b + ai - bi = 8$$

Thus $a = 2, b = 2$ and the general solution is $u_n = 2(2 + i)^n + 2(2 - i)^n$