

# Solving discrete problems — Math 2020, Spring 2005

**Schedule** For Tuesday, February 15, 2005.

1. Unique prime factorisation in the integers:  
(see page 126 or <http://www.maths.monash.edu.au/mth3122/a4lect3.pdf> )
2. Modular arithmetic. (Also called congruences. Section 3.6 of book.)
3. Fermat's little theorem.  
This gives a quicker way to tell if a number is prime. See page 411, Theorem 10.29 in text book.

## Quiz

Next Thursday the quiz will be on modular arithmetic, with questions like:

Find  $4 \times 6 \pmod{7}$ , or find  $4/5 \pmod{7}$ .

The answer should be 0, 1, 2, 3, 4, 5 or 6 in each case.

About 3 or 4 such questions would be on the quiz.

**Homework** Due Tuesday February 22.

1. Make multiplication and division tables for the integers modulo  $n$  for  $n = 2, 3, 4, 5, 6, 7, 8$ .

Example, for  $n = 7$ , make two tables, one for  $a \times b$  and one for  $a/b$ . A couple of entries are filled in here:

a	b						
	0	1	2	3	4	5	6
0							
1							
2						3	
3							
4							
5							
6							2

Table for  $a \times b$

a	b						
	0	1	2	3	4	5	6
0							
1							
2						6	
3							
4							
5							
6							

Table for  $a/b$

Example: in the table  $2 \times 5 = 10 \equiv 3 \pmod{7}$ .

To find  $2/5 \pmod{7}$ , if  $2/5 \equiv x \pmod{7}$ , this means  $2 \equiv x \times 5 \pmod{7}$ .

Once you've filled in the multiplication table, you can see that  $6 \times 5 \equiv 2 \pmod{7}$ , so we can write  $2/5 \equiv 6 \pmod{7}$ .

For some examples,  $a/b \pmod{n}$  might not exist.

In this case, just draw a line (—) in the space in the table instead of a number.

2. For an integer  $n$ , we define  $\mathbf{Z}/n\mathbf{Z}$  to be the set of integers modulo  $n$ , so we can write  $\mathbf{Z}/n\mathbf{Z} = \{0, 1, 2, \dots, n-1\}$ .

The rules of addition on  $\mathbf{Z}/n\mathbf{Z}$  are modulo  $n$ .

Now we set

$$\mathbf{Z}/n\mathbf{Z}^\times = \{x : x \in \mathbf{Z}/n\mathbf{Z} \text{ and } \gcd(x, n) = 1\}.$$

Here the gcd is computed in the usual way as for integers.

A. Prove the following result:

If  $n, a$  and  $b$  are integers, and if  $a \equiv b \pmod{n}$ , then  $\gcd(a, n) = \gcd(b, n)$ .

B. Find the number of elements in  $\mathbf{Z}/n\mathbf{Z}^\times$  for  $n = 2, 3, 4, 5, 6, 7, 8, 9, 10$ .

Note, if  $A$  is a set, the number of elements in  $A$  is usually written as  $\#A$  or  $|A|$ . E.g.,  $\#(\mathbf{Z}/11\mathbf{Z})^\times = 10$ .

C. Prove that if  $p$  is prime, then  $\mathbf{Z}/p\mathbf{Z}^\times$  has  $p-1$  elements.

D. What can you say about the number of elements in  $\mathbf{Z}/n\mathbf{Z}^\times$  when  $n$  is not prime?

E. Find the number of elements in  $(\mathbf{Z}/2^n\mathbf{Z})^\times$  for  $n = 1, 2, 3, 4$  do you notice a pattern?

F. Find the number of elements in  $(\mathbf{Z}/(3 \times 5)\mathbf{Z})^\times$ ,  $(\mathbf{Z}/(2 \times 5)\mathbf{Z})^\times$  and  $(\mathbf{Z}/(3 \times 7)\mathbf{Z})^\times$ . Do you notice any pattern? How many elements do you think are in  $(\mathbf{Z}/(p \times q)\mathbf{Z})^\times$  for  $p$  and  $q$  primes, with  $p \neq q$ .

G. For integers  $n, a$ , find a condition on  $a$  so that  $1/a \pmod{n}$  exists.

(To spot a pattern, use the tables computed in question 1, and more tables if necessary).

3. Can you find an example of a number  $m$ , which is not prime, and another number  $a$  so that  $a^{m-1} \equiv 1 \pmod{m}$ ? Is so, give an example, if not, why not?

If  $a^{m-1} \equiv 1 \pmod{m}$  for all  $a$  with  $1 \leq a \leq m-1$ , can we conclude that  $m$  is prime? If so, prove this, if it's not true, give an example.

# Unique Prime Factorisation of integers

## Statement of the Theorem:

Let  $x$  be an integer greater than 1.

If $x = p_1^{m_1} \cdot p_2^{m_2} \cdots p_r^{m_r}$ , and $x = q_1^{n_1} \cdot q_2^{n_2} \cdots q_s^{n_s}$
---

then

$r = s$ , and the $p_i$ and $q_j$ are the same in some order, and if $p_i = q_j$ , then $m_i = n_j$ .
---

### IMPORTANT:

There are some more hypothesis we need about  $p_i$ ,  $q_j$ ,  $m_i$ ,  $n_j$  and  $r$  and  $s$  in the statement of this theorem. What are they?

## Proof of unique prime factorisation of the integers:

The proof we will look at has the following basic structure:

	Statement of theorem: $P \wedge Q$	$\rightarrow$	$R \wedge S \wedge T$	reason
	Proof:			
1.	$P$	$\rightarrow$	$P_1$	arithmetic
2.	$P_1$	$\rightarrow$	$A_1$	definition
3.	$A_1 \wedge Q$	$\rightarrow$	$B_1$	previous result
4.	$C_1 \vee D_1 \vee E_1$			fact about integers
5.	$C_1 \wedge P \wedge Q$	$\rightarrow$	False (Contradiction)	arith. & previous result
6.	$D_1 \wedge P \wedge Q$	$\rightarrow$	False (Contradiction)	arith. & previous result
7.	$\therefore P \wedge Q$	$\rightarrow$	$E_1$	logic (from 4—6)
8.	$\therefore P \wedge Q$	$\rightarrow$	$B_1 \wedge E_1$	logic (from 1—3 and 7)
9.	$P \wedge Q$	$\rightarrow$	$B_2 \wedge E_2 \wedge \dots B_r \wedge E_r$	same as above
10.	$P \wedge Q$	$\rightarrow$	$G_1 \wedge G_2 \dots G_s$	same as above
11.	$B_1 \wedge \dots \wedge B_r$	$\rightarrow$	$U$	counting
12.	$G_1 \wedge \dots \wedge G_s$	$\rightarrow$	$V$	counting
13.	$U \wedge V$	$\rightarrow$	$R$	fact about integers
14.	$B_1 \wedge \dots B_r \wedge G_1 \wedge \dots \wedge G_s$	$\rightarrow$	$S$	restatement
15.	$E_1 \wedge \dots \wedge E_r$	$\rightarrow$	$T$	restatement
16.	$P \wedge Q$	$\rightarrow$	$R \wedge S \wedge T$	logic (from lines 8 — 15)

Q.E.D.

The reasons for the steps come from the following:

1) Basic definitions and arithmetic

— you should be able to work out the arithmetic, and what definitions are used in these steps.

2) The integers are totally ordered.

This means that for any two integers  $a$  and  $b$ , either  $a < b$ ,  $a > b$  or  $a = b$ . There are no other possibilities.

3) The “previous results” used come from previous lectures, especially the last lecture, so should be results from the following list:

**Theorem 1** Let  $p$  be a prime and let  $a$  and  $b$  be positive integers. Then if  $p|ab$  then  $p|a$  or  $p|b$

**Theorem 2** Let  $p$  be a prime and let  $r$  be a positive integer, and let  $a_1, a_2, \dots, a_r$  be positive integers.

Then if  $p|a_1 \times \dots \times a_r$  then  $p|a_i$  for some  $i$  with  $1 \leq i \leq r$ .

**Theorem 3** Let  $p$  be a prime and let  $r$  be a positive integer, and let  $a$  be a positive integer.

Then if  $p|a^r$  then  $p|a$ .

### Theorem 4

If  $p$  is a prime, and if  $r$  is an integer, with  $r \geq 1$ , and if  $a_1, a_2, \dots, a_r$  are positive integers, and  $m_1, m_2, \dots, m_r$  are positive integers,

then if  $p$  divides  $a_1^{m_1} \times \dots \times a_r^{m_r}$  then  $p|a_i$  for some  $i$  with  $1 \leq i \leq r$ .

(Note, the product  $a_1^{m_1} \times \dots \times a_r^{m_r}$  can also be written as  $\prod_{j=1}^r a_j^{m_j}$ .)

### Theorem 5

If  $p$  and  $q$  are primes, then if  $p|q$  then  $p = q$ .

### Theorem 6

If  $p$  is a prime, and if  $r$  is an integer, with  $r \geq 1$ , and if  $q_1, q_2, \dots, q_r$  are prime numbers, and  $m_1, m_2, \dots, m_r$  are positive integers,

then if  $p$  divides  $\prod_{j=1}^r q_j^{m_j}$  then  $p = q_i$  for some  $i$  with  $1 \leq i \leq r$ .