# *Discrete Mathematics (Part A)*

UNIVERSITY OF
CAMBRIDGE
Computer Laboratory

*Computer Science Tripos Part 1A*
*Mathematics Tripos 1A (CS Option)*

*Peter Robinson*

*Michaelmas 2001*

William Gates Building
JJ Thomson Avenue
Cambridge
CB3 0FD

http://www.cl.cam.ac.uk/

# Introduction

This course will develop the idea of formal proof by way of examples involving simple objects such as integers and sets. The material enables academic study of Computer Science and will be promoted with examples from the analysis of algorithms and cryptography.

## Syllabus

These notes cover the first half of the course.

### Integers

- Proof. Deduction, contradiction. Integers, mathematical induction. [2 lectures]
- Factors. Division: highest common factors and least common multiples. Euclid's algorithm: solution in integers of $ax + by = c$, the complexity of Euclid's algorithm. Euclid's proof of the infinity of primes. Existence and uniqueness of prime factorisation. Irrationality of $\sqrt{p}$; brief discussion of rational and algebraic numbers. [3 lectures]
- Modular arithmetic. Solving congruences. Units modulo $m$, Euler's totient function. Wilson's theorem. Chinese remainder theorem. The Fermat-Euler theorems. Public key cryptography. [3 lectures]

## Objectives

On completing this half of the course, students should be able to:

- Write a clear statement of a problem as a theorem in mathematical notation.
- Prove and disprove assertions using a variety of techniques.
- Describe, analyse and use Euclid's algorithm.
- Explain and apply prime factorisation.
- Perform calculations with modular arithmetic.
- Use number theory to explain public key cryptography.

# *Appropriate books*

The following books are relevant for the course:

- NL Biggs: *Discrete Mathematics,* Oxford University Press, 1989, ISBN 0-19-853427-2, £22.95.
- JH Conway & RK Guy: *The book of numbers,* Springer-Verlag, 1996, ISBN 0-387-97993-X, £21.95  
A beautiful book – deeply subtle mathematics presented in an accessible and exciting way.
- H Davenport: *The higher arithmetic* (6th edition), Cambridge University Press, 1992, ISBN 0-521-42227-2, £14.95.
- P Giblin: *Primes and programming,* Cambridge University Press, 1993, ISBN 0-521-40988-8, £15.95.
- RL Graham, DE Knuth and O Patashnik: *Concrete mathematics* (2nd edition), Addison Wesley, 1994, ISBN 0-201-55802-5, £26.00.  
The ultimate reference book.
- JF Humphreys and MY Prest: *Numbers, groups and codes,* Cambridge University Press, 1989, ISBN 0-521-35938-4, £14.95.  
Close to the approach in this course.
- HF Mattson: *Discrete Mathematics,* Wiley, 1993, ISBN 0-471-59966-2, £21.95.
- N Nissanke: *Introductory logic and sets for Computer Scientists*, Addison-Wesley, 1999, ISBN 0-201-17957-1, £20.95.
- G Pólya: *How to solve it,* Penguin, 1990, ISBN 0-14-012499-3, £8.99.
- KH Rosen: *Discrete mathematics and its applications* (4th edition), McGraw-Hill, 1999, IBN 0-07-116756-0, £23.99.  
An excellent book covering a wide range of topics and useful throughout the course.

These notes do not constitute a complete transcript of all the lectures and they are not a substitute for text books. They are intended to give a reasonable synopsis of the subjects discussed, but they give neither complete proofs of all the theorems nor all the background material.

# Proof

What is a proof? If a theorem is a logical statement, the proof is meant to convince you that the statement is true. When faced with a proof you should convince yourself of three things:

- The arguments put forward are all true and the sequence follows logically from beginning to end.
- The arguments are sufficient to prove the theorem.
- The arguments are all necessary to prove the theorem.

A proof has to encompass all the possible cases permitted by the statement of the proof. Usually it will not be possible to work through all of these in turn, so some generality will be required. On the other hand, a single counter-example *is* sufficient to show that a theorem is false. Indeed, such a counter-example should be as simple as possible. Good mathematicians like to avoid effort.

This should not be confused with proof by contradiction. This is an elegant technique in which we prove a theorem by accepting the possibility that it is not true. If it is not true, there must be a counter-example. Examining this counter-example then gives rise to a logical inconsistency. If all the intermediate steps are correct, the only explanation is that the original assumption (accepting that the theorem was not true) was itself mistaken. In other words, the theorem *is* true.

## Examples

1. **Theorem**: $a^n + b^n = c^n$ has no solutions.

   **Proof:** Left as an exercise for the reader.

2. **Theorem:** The whole numbers that can be expressed as the difference of two squares are precisely those that leave a remainder of $0$, $1$ or $3$ when divided by $4$.

   **Proof:** Work through a sequence of simpler problems.

   a) Any odd number can be expressed as the difference of two squares – consider $(n+1)^2 – n^2$.

   b) No even number can be expressed as the difference of two squares – false, consider $4 = 2^2 – 0^2$.

   c) Any exact multiple of 4 can be expressed as the difference of two squares – consider $(n+1)^2 – (n–1)^2$.

   d) No odd multiple of two can be expressed as the difference of two squares – assume true and find a contradiction by examining cases.

   Now combine these results. (d) shows that any difference of two squares leaves a remainder of $0$, $1$ or $3$ when divided by $4$. (a) shows that a number that leaves remainder $0$ when divided by $4$ can be expressed as the difference of two squares, and (c) shows that a number that leaves a remainder of $1$ or $3$ can.

3. **Theorem:** $\sqrt{2}$ is *irrational*, that is, it can not be written as a fraction $\frac{x}{y}$ for whole numbers $x$ and $y$.

   **Proof:** Assume that $\sqrt{2} = \frac{x}{y}$ for whole numbers $x$ and $y$. Without loss of generality, we can assume that $x$ and $y$ are not both even and deduce a contradiction.

# *How to solve it*

Pólya suggests the following four step plan for problem solving:

## Understanding the problem

What is the unknown?  What are the data?  What is the condition?

Is it possible to satisfy the condition?  Is the condition sufficient to determine the unknown?  Or is it insufficient?  Or redundant?  Or contradictory?

Draw a figure.  Introduce suitable notation.

Separate the various parts of the condition.  Can you write them down?

## Devising a plan

Find the connection between the data and the unknown.  You may be obliged to consider auxiliary problems if an immediate connection cannot be found.  You should obtain eventually a plan of the solution.

Have you seen it before?  Or have you seen the same problem in a slightly different form?

Do you know a related problem?  Do you know a theorem that could be useful?

Look at the unknown!  And try to think of a familiar problem having the same or a similar unknown.

Here is a problem related to yours and solved before.  Could you use it?  Could you use its results?  Could you use its method?  Should you introduce some auxiliary element in order to make its use possible?

Could you restate the problem?  Could you restate it still differently?  Go back to definitions.

If you cannot solve the proposed problem try to solve first some related problem.  Could you imagine a more accessible related problem?  A more general problem?  A more special problem?  An analogous problem?  Could you solve a part of the problem?  Keep only a part of the condition, drop the other part; how far is the unknown then determined, how can it vary?  Could you derive something useful from the data?  Could you think of other data appropriate to determine the unknown?  Could you change the unknown or data, or both if necessary, so that the new unknown and the new data are nearer to each other?

Did you use all the data?  Did you use the whole condition?  Have you taken into account all essential notions involved in the problem?

## Carrying out the plan

Carrying out your plan of the solution, check each step.  Can you see clearly that the step is correct?  Can you prove that it is correct?

## Looking back

Can you check the result?  Can you check the argument?

Can you derive the result differently?  Can you see it at a glance?

Can you use the result, or the method, for some other problem?

# Integers

We start with the sets of natural numbers, $\mathbb{N} = \{1, 2, 3, \ldots\}$, the natural numbers augmented with $0$, $\mathbb{N}_0 = \{0, 1, 2, \ldots\}$, and integers, $\mathbb{Z} = \{\ldots, -2, -1, 0, 1, 2, \ldots\}$, and will refer to the rational numbers (fractions), $\mathbb{Q}$, and the real numbers $\mathbb{R}$. The curly brackets just wrap up enumerations of elements. We will set out the notation for sets more formally in the second half of the course, but here is enough to get started.

A particular value, $x$, is an *element* of a set $X$ if it is in it. We write this with a sort of Greek epsilon: $x \in X$. So $-3 \in \mathbb{Z}$ but $-3 \notin \mathbb{N}$.

One set, $X$, is a *subset* of another set, $Y$, if every element of $X$ is also an element of $Y$. We write this with a rounded less-than-or-equal sign: $X \subseteq Y$. So $\mathbb{N} \subseteq \mathbb{N}_0 \subseteq \mathbb{Z} \subseteq \mathbb{Q} \subseteq \mathbb{R}$.

We can also define sets by *predicates* or conditions: $\mathbb{N} = \{x \in \mathbb{Z} \mid x > 0\}$. This notation is a bit unfortunate because we will also use the vertical bar to indicate exact divisibility: 3 **|** 6. So the set of even numbers might be defined as $E = \{x \in \mathbb{Z} \mid 2|x\}$, which is a bit confusing. Sorry.

There are two particularly important properties of the natural numbers, which turn out to be equivalent: induction and well-ordering.

## Mathematical induction

Let $P(n)$ be any mathematical assertion involving the natural number $n$ which may be true or false. (Think of $P$ as a function with $n$ as an argument and returning a Boolean result.) If

1. $P(1)$ is true, and
2. whenever $P(k)$ is true then $P(k+1)$ is true as well

then $P(n)$ is true for every natural number $n$.

The two conditions are known as the *base case* and the *inductive step*, and they give rise to the *conclusion*.

### Examples

1. $1 + 2 + 3 + \cdots + n = \frac{1}{2}n(n+1)$.
2. Let $a_n = 2^{3n+1} + 3^{n+1}$. Then, for all positive integers $n$, $a_n$ is exactly divisible by $5$.
3. If $n$ is a positive integer and $x$ and $y$ are any numbers, then
$$(x+y)^n = \binom{n}{0}x^n + \binom{n}{1}x^{n-1}y^1 + \cdots + \binom{n}{i}x^{n-i}y^i + \cdots + \binom{n}{n}y^n$$
where $\binom{n}{k}$ is the *binomial coefficient*, defined to be $\dfrac{n!}{k!(n-k)!}$.

## Well ordering

Any non-empty subset of $\mathbb{N}$ contains a smallest element.

That may seem obvious, but it is not true for the integers, rationals or reals. It is also an important property that will extend to other sets where each element does not have a natural successor and so ordinary induction can not be used. However, some sort of ordering relation ≤ is still necessary.

# Equivalence

Well-ordering implies mathematical induction.

## Proof

Suppose that the assertion $\mathrm{P}(n)$ satisfies the two conditions for mathematical induction. So $\mathrm{P}(1)$ is true and $\mathrm{P}(k)$ implies $\mathrm{P}(k+1)$. We need to show that $\mathrm{P}(n)$ is true for every natural number $n$.

The proof starts rather surprisingly. We give up and suppose that we can not manage it. In other words we suppose that there are some natural numbers $n$ for which $\mathrm{P}(n)$ is false. These counter-examples are going to be interesting, so gather them all together in a set. Let $\mathrm{S} = \{x \in \mathbb{N} \mid \mathrm{P}(x) \text{ is false}\}$. If $\mathrm{S}$ is empty then there are no counter-examples, so $\mathrm{P}(n)$ was true for every natural number $n$ after all.

If $\mathrm{S}$ is not empty then, by well-ordering, it contains a least element. Call it $s$. Now $s \neq 1$ since the base case said that $\mathrm{P}(1)$ was true and so $1 \notin \mathrm{S}$. Therefore $s > 1$ and $s-1 \in \mathbb{N}$. Moreover, $\mathrm{P}(s-1)$ must be true since $s$ was the smallest counter-example. But the inductive step now says that $\mathrm{P}(s)$ must be true and so $s \notin \mathrm{S}$.

This is a contradiction, so something has gone wrong. The only possibility is our original supposition that the theorem was not true. In other words, $\mathrm{S}$ is empty and $\mathrm{P}(n)$ is true for every natural number $n$.

# Exercises

1. Prove that $1^2 + 2^2 + 3^2 + \cdots + n^2 = \frac{1}{6} n(n+1)(2n+1)$.

2. Find the sum of the first $n$ cubes. Calculate the first few cases, formulate a general rule and confirm it by induction.

3. Evaluate the sum $\frac{1}{2!} + \frac{2}{3!} + \frac{3}{4!} + \cdots + \frac{n}{(n+1)!}$.

4. Show that $7$ divides $2^{4n+2} + 3^{2n+1}$ and $13$ divides $3^{n+1} + 4^{2n\text{-}1}$ for all natural numbers $n$.

5. The *Fibonacci* numbers are defined by $f_0 = 0, f_1 = 1$ and $f_n = f_{n-1} + f_{n-2}$ for $n > 1$.

   Show that $f_n = \frac{1}{\sqrt{5}}\left(\left(\frac{1+\sqrt{5}}{2}\right)^n - \left(\frac{1-\sqrt{5}}{2}\right)^n\right)$ for all $n \geq 0$.

6. Prove that, for all $n \in \mathbb{N}_0$ and $x \in \mathbb{R}$ with $x \geq \text{-}1$, $(1 + x)^n \geq 1 + n\,x$.

7. A *triomino* is an L-shaped pattern made from three square tiles. A $2^k \times 2^k$ chessboard, whose squares are the same size as the tiles, has an arbitrary square painted purple. Show that the chessboard can be covered with triominoes so that only the purple square is exposed.

   *Hint:* Use induction. The base case has $k = 1$ and the inductive step requires you to find four similar but smaller problems.

8. A prison houses $100$ inmates, one in each of $100$ cells, guarded by a total of $100$ warders. One evening, all the cells are locked and the keys left in the locks. As the first

warder leaves, she turns every key, unlocking all the doors. The second warder turns every second key, re-locking every even numbered cell. The third warder turns every third key and so on. Finally the last warder turns the key in just the last cell. Which doors are left unlocked and why?

*Hint:* This is a question about division.

9. [Mathematical Tripos Part 1A 1988, Paper 6, Question 9]

   State the principle of mathematical induction. Prove your statement, assuming that every non-empty subset of the natural numbers contains a least element.

   The Master of Regents' College and his wife invite $n$ Fellows and their spouses to a party. After the party the Master asks everyone (including his own wife) how many people they shook hands with, and receives $2n + 1$ different answers. Of course, no woman shook hands with her own husband. Show that the person who shook the most hands was not the Master's wife.

   How many hands did the Master shake?

   *Hint:* Consider the largest and smallest numbers of people with whom a guest could shake hands. What does this tell you about the answers that the Master received? What does this tell you about the relationship between the person who shook most hands and the person who shook least?

   *Another hint:* The last part of the question is about induction.

10. Complete the proof of equivalence by using induction to prove that the natural numbers are well-ordered.

    *Hint:* Use contradiction. Suppose that $\mathrm{X}$ is a set of natural numbers which contains no least element. You need to prove that $\mathrm{X}$ is empty. Let $\mathrm{L}$ be the set of natural numbers $n$ such that $n$ is not greater than or equal to any element in $\mathrm{X}$. Show by induction that $\mathrm{L}$ is the set of natural numbers, so $\mathrm{X}$ is, indeed, empty.

11. [Not to be taken too seriously.] Comment on the following alleged proofs by induction (with acknowledgements to Professor JWS Cassels):

    - Let $n$ be a natural number and $a_j$ be real numbers for $1 \le j \le n$. Then $a_j = a_k$ for $1 \le j \le n$, $1 \le k \le n$.

      **Proof** Certainly true for $n = 1$. Assume the result is true for $n$ and prove it for $n+1$. By case $n$ of the result, we have $a_1 = a_2 = \cdots = a_n$. Applying this to the $a_{j+1}$ instead of the $a_j$ we have $a_2 = \cdots = a_n = a_{n+1}$. Hence $a_1 = a_2 = \cdots = a_n = a_{n+1}$, which is the result for $n+1$.

    - Every natural number $n$ is interesting.

      **Proof** There certainly are some interesting natural numbers: 0 is the smallest, 1 is the only natural number whose reciprocal is a natural number, 2 is the smallest prime, 3 is the number of persons in the Trinity, and so on. So, if the statement were false, there would be a smallest natural number $n$ which is not interesting. This is a contradiction, since $n$ would be a very interesting number indeed.

    - Every odd integer > 1 is prime.

      **Proof** The economist's proof runs as follows. 3 is prime, 5 is prime, 7 is prime. Three cases in a row is surely enough.

      If, however, we imagine an idealised economist who would not be satisfied by this, then the rest of the proof would continue as follows: Look at the next odd integer, 9. Well, it is admittedly not a prime; there must be some unusual factor of some kind operating. Let's go on looking at the figures. 11 is prime, 13 is prime. Two more confirmations, so it must be true.

- Every prime is odd.

  **Proof** $3, 5, 7, 11, 13, 17, 19, \ldots$ are all odd. There only remains $2$, which must be the oddest prime of all.

- $n^2 - n + 41$ is prime for all natural numbers *n*.

  **Proof** The physicist's proof runs as follows. Write a computer program to check successively that $n^2 - n + 41$ is prime for $n = 0, 1, 2, \ldots 30$. Since quite a number of cases have now been verified using very expensive equipment, the result must be true.

# Factors

The operations of addition, multiplication and ordering on the integers have some useful properties.

## Division

Given integers $a$ and $b$, we say that $a$ *divides* $b$ or $a$ is a *factor* of $b$ (written $a \mid b$) if $b = qa$ for some integer $q$. Moreover, $a$ is a *proper divisor* of $b$ if $a \mid b$ and $a \neq \pm 1 \text{ or } \pm b$.

- If $a \mid b$ and $b \mid c$ then $a \mid c$.
- If $d \mid a$ and $d \mid b$ then $d \mid (ax + by)$ for any integers $x$ and $y$.

## Division algorithm

Given $a, b \in \mathbb{N}$, there exist unique integers $q$ and $r$ with $a = bq + r$ and $0 \leq r < b$. $q$ is called the *quotient* and $r$ is the *remainder* after dividing $a$ by $b$. The latter is written as $a \bmod b$ or, sometimes, as $a$ % $b$. So $b \mid a$ if, and only if, $r = 0$, that is, $a \bmod b = 0$.

**Proof:** Consider $\mathrm{R} = \{a - bk \mid k \in \mathbb{Z}$ and $(a - bk) \geq 0\}$.

This is not actually an algorithm in the normal sense understood by computer scientists, but there are algorithms that implement division in hardware or software. The important mathematical result is the existence and uniqueness of quotients and remainders.

## Highest common factors

Given $a, b \in \mathbb{N}$, the *highest common factor* (*HCF*) or *greatest common divisor* (*GCD*) of $a$ and $b$, written as $(a, b)$, is defined to be $d \in \mathbb{N}$ satisfying:

1. $d \mid a$ and $d \mid b$, and
2. if $e \mid a$ and $e \mid b$ then $e \mid d$.

The second condition implies that $e \leq d$, but is a more general expression that allows the proofs that follow to be extended easily into sets other than the integers.

This definition has several consequences:

- The HCF exists and is unique.

  **Proof:** Consider the least element of $\mathrm{D} = \{as + bt \mid s, t \in \mathbb{Z}$ and $(as + bt) > 0\}$.

- There are integers $x$ and $y$ with $d = ax + by$. Moreover, $x$ and $y$ can be calculated efficiently.
- If $a, b \in \mathbb{N}$ and $a = bq + r$ for integers $q$ and $r$ with $0 \leq r < b$, then $(a, b) = (b, r)$. This will give rise to an efficient algorithm for HCFs.
- If $a \mid bn$ and $(a, b) = 1$, then $a \mid n$.
- If $a \mid n$, $b \mid n$ and $(a, b) = 1$, then $ab \mid n$.
- $\left( \dfrac{a}{(a,b)}, \dfrac{b}{(a,b)} \right) = 1$

We say that $a$ and $b$ are *co-prime* if $(a, b) = 1$.

The *lowest common multiple* of $a$ and $b$ is the smallest number $m$ which is exactly divisible by both $a$ and $b$. This is sometimes written as $[a, b]$ and is equal to $ab \div (a, b)$.

# *Euclid's algorithm*

Given $a, b \in \mathbb{N}$, use the division algorithm to write:

$$\begin{array}{rll} a = & q_1 b + r_1 & 0 \le r_1 < b \\ b = & q_2 r_1 + r_2 & 0 \le r_2 < r_1 \\ r_1 = & q_3 r_2 + r_3 & 0 \le r_3 < r_2 \\ & \dots & \\ r_{i-2} = & q_i r_{i-1} + r_i & 0 \le r_i < r_{i-1} \\ & \dots & \\ r_{n-2} = & q_n r_{n-1} & \text{with remainder } r_n = 0 \end{array}$$

Then $(a, b) = (b, r_1) = (r_1, r_2) = \dots = (r_{n-1}, r_{n-2}) = r_{n-1}$.

Moreover, we can now work backwards through the algorithm to calculate the integers $x$ and $y$ with $(a, b) = ax + by$.

Alternatively, we can produce the same result working forwards by observing that line $i$ is just the difference of line $i–2$ and $q_i$ times line $i–1$. Write $r_{-1} = a$ and $r_0 = b$, so $q_i$ is just the integer quotient of $r_{i-2}$ divided by $r_{i-1}$. Now express $r_i = s_i a + t_i b$ so $s_{-1} = 1$, $t_{-1} = 0$, $s_0 = 0$ and $t_0 = 1$ and observe that $r_i = r_{i-2} - q_i r_{i-1}$, $s_i = s_{i-2} - q_i s_{i-1}$ and $t_i = t_{i-2} - q_i t_{i-1}$.

Here is a worked example:

| $i$ | $q_i$ | $r_i$ | | $s_i$ | $t_i$ |
|---|---|---|---|---|---|
| | | $a = 55$ | $= 2.20 + 15$ | 1 | 0 |
| | | $b = 20$ | $= 1.15 + 5$ | 0 | 1 |
| 1 | 2 | 15 | $= 3.5 + 0$ | 1 | -2 |
| 2 | 1 | 5 | | -1 | 3 |
| 3 | 3 | 0 | | 4 | -11 |

The last line tells us that $4.55 - 11.20 = 0$ so $4k.55 - 11k.20 = 0$. This is rather like the finding the complementary function that solves the homogeneous part of a differential equation.

The penultimate line tells us that $(55, 20) = 5 = -1.55 + 3.20$. This is rather like finding the particular solution for an inhomogeneous differential equation.

## Observations

- The signs of $s_i$ alternate $1\ 0\ 1 - + - \dots$ and those of $t_i$ alternate $0\ 1 - + - + \dots$.

  **Proof:** $a$, $b$ and all the remainders $r_i$ are positive, so the quotients $q_i$ will be as well.

- $s_{i-1}t_i - s_i t_{i-1} = (-1)^i$ for $i \ge 0$, so, in particular, $s_i$ and $t_i$ are co-prime.

  **Proof:** By induction.

- $|s_n| = \dfrac{b}{(a,b)}, |t_n| = \dfrac{a}{(a,b)}$.

  **Proof:** Note that $r_n = s_n a + t_n b = 0$ and divide through by $(a, b)$.

### Applications

- Given $a, b, c \in \mathbb{Z}$ with $a$ and $b$ not both zero, the linear Diophantine equation $ax + by = c$ has a solution with $x, y \in \mathbb{Z}$ if, and only if, $(a, b) \mid c$.

  Moreover, any solution to $au + bv = c$ has $u = x + \frac{kb}{(a,b)}$ and $v = y - \frac{ka}{(a,b)}$ for some $k \in \mathbb{Z}$. The general solution is just the sum of the particular solution $u = x$ & $v = y$ with the complementary function $u = \frac{kb}{(a,b)}$ & $v = -\frac{ka}{(a,b)}$ where $k$ is an arbitrary constant.

- $a \div b$ can be written as the continued fraction $q_1 + \cfrac{1}{q_2 + \cfrac{1}{q_3 + \cdots}} = q_1 + \frac{1}{q_2 +}\frac{1}{q_3 +}\cdots$.

### Efficiency

If $a > b$ and $b$ has $d$ digits (to the base $10$), then Euclid's algorithm will take at most $5d + 2$ steps to find $(a, b)$.

It is actually rather hard to say how many steps will be required for any given pair of numbers. So we follow Pólya's advice and ask a different question. What is the smallest number that will require $n$ steps? This will arise when $q_i = 1$ for $1 \le i < n$ and $q_n = 2$.

Using the earlier notation, $|s_i| = |s_{i-1}| + |s_{i-2}|$ and $|t_i| = |t_{i-1}| + |t_{i-2}|$ so $|s_i| = f_i$ and $|t_i| = f_{i+1}$ where $f_i$ is the $i^{\text{th}}$ Fibonacci number. So, if $b < f_n$, $|s_n| < f_n$ and we need fewer than $n$ steps.

However, if $n = 5d + 2$, then $f_n > 1.6^{n-2} = 1.6^{5d} > 10^d > b$, as required.

## Primes

A natural number $p$ is *prime* if $p > 1$ and $p$ has no proper divisor.

### Digression

- $2^{2976221} - 1$ is prime.
- The Mersenne number $2^n - 1$ is prime only when $n$ is prime, but that is not sufficient.
- The Fermat number $2^n + 1$ is prime only when $n$ is of the form $2^m$, but that is not sufficient.
- If $p$ is a Fermat prime, then it is possible to construct a regular $p$–gon using only pencil, ruler and compasses.

### Observations

- If $p$ is a prime and $p \mid ab$ for $a, b \in \mathbb{N}$ but not $p \mid a$ then $p \mid b$.
- There are infinitely many primes.
- If $p$ is a prime then $\sqrt{p}$ is irrational; that is, it can not be expressed as a ratio of two natural numbers.
- Let $\Pi(x)$ be the number of primes $\le x$. Then $\Pi(x) \approx x / \ln x$.
- *Prime pair conjecture:* There are infinitely many primes $p$ with $p + 2$ also prime.

- *Goldbach conjecture:* Every even integer greater than $2$ can be expressed as the sum of two primes.

### Fundamental theorem of arithmetic

Every natural number greater than 1 can be expressed as a product of primes. Moreover, the expression is unique up to the order of the primes.

**Proof:** By contradiction.

### Observation

- If $m = p_1^{r_1} p_2^{r_2} \ldots p_k^{r_k}$ and $n = p_1^{s_1} p_2^{s_2} \ldots p_k^{s_k}$ then $(m, n) = p_1^{\min(r_1,s_1)} p_2^{\min(r_2,s_2)} \ldots p_k^{\min(r_k,s_k)}$.

## *Exercises*

1. Are the following statements true or false?
   - $(a, b)\,(c, d) = (ac, bd)$
   - $(a, b)\,(a, d) = (a^2, bd)$
   - $(a, b) = (a, d) = 1$ implies that $(a, bd) = 1$
2. Prove that, if $x$ and $y$ are integers such that $57x + 44y = 1$, then there is an integer $k$ such that $x = 17 - 44k$ and $y = 57k - 22$.
3. Does the equation $1992x + 1752y = 12$ have a solution in integers? Find all the integer solutions to the equation $1992x + 2622y = 12$.
4. Find integers $x$, $y$ and $z$ such that $56x + 63y + 72z = 1$.
5. A photocopier charges 7.2p for each copy. However, it only accepts 10p coins and gives no change, although unused credit is carried forward. What is the smallest number of copies that must be made if the user is not to forgo any change?
6. Show that there are infinitely many prime numbers of the form $4k + 3$. [*Hint:* Consider $N = 2^2.3.5.7.\ldots.p_n - 1$.]
7. Write an ML function to factor an integer into a list of prime factors.
8. Write an ML function to implement Euclid's algorithm. Given two integers $a$ and $b$, this should return a triple $(x, y, z)$ such that $ax + by = z$ where $z$ is the greatest common divisor of $a$ and $b$.
9. Recall the Fibonacci numbers $\{f_n\}$. Show, by induction on $k$ or otherwise, that $f_{n+k} = f_k f_{n+1} + f_{k-1} f_n$. Deduce that $f_n \mid f_{ln}$ for all $l \geq 1$. Deduce also that $(f_m, f_n) = (f_{m-n}, f_n)$ and hence that $(f_m, f_n) = f_{(m,\,n)}$. Show that $f_m f_n \mid f_{mn}$ if $(m, n) = 1$.

# Modular arithmetic

If $a, b \in \mathbb{Z}$ and $m \in \mathbb{N}$ then we say that $a$ and $b$ are *congruent modulo $m$* if $m \mid (a - b)$, and we write this as $a \equiv b \pmod{m}$.

This equivalent to saying that there is $q \in \mathbb{Z}$ such that $a = b + qm$.

## Observations

- For all $a \in \mathbb{Z}$ and $m \in \mathbb{N}$ we have $a \equiv a \pmod{m}$.
- If $a \equiv b \pmod{m}$ then $b \equiv a \pmod{m}$.
- If $a \equiv b \pmod{m}$ and $b \equiv c \pmod{m}$, then $a \equiv c \pmod{m}$.
- If $a_1 \equiv b_1 \pmod{m}$ and $a_2 \equiv b_2 \pmod{m}$ then $a_1 + a_2 \equiv b_1 + b_2 \pmod{m}$ and $a_1a_2 \equiv b_1b_2 \pmod{m}$.
- However, $a \equiv b \pmod{m}$ does *not* imply that $x^a \equiv x^b \pmod{m}$. For example, consider $a = 1$, $b = 4$, $m = 3$, and $x = 2$.

## Examples

Here are the addition and multiplication tables modulo 4:

| + | 0 | 1 | 2 | 3 |
|---|---|---|---|---|
| 0 | 0 | 1 | 2 | 3 |
| 1 | 1 | 2 | 3 | 0 |
| 2 | 2 | 3 | 0 | 1 |
| 3 | 3 | 0 | 1 | 2 |

| × | 0 | 1 | 2 | 3 |
|---|---|---|---|---|
| 0 | 0 | 0 | 0 | 0 |
| 1 | 0 | 1 | 2 | 3 |
| 2 | 0 | 2 | 0 | 2 |
| 3 | 0 | 3 | 2 | 1 |

and multiplication modulo 5:

| × | 0 | 1 | 2 | 3 | 4 |
|---|---|---|---|---|---|
| 0 | 0 | 0 | 0 | 0 | 0 |
| 1 | 0 | 1 | 2 | 3 | 4 |
| 2 | 0 | 2 | 4 | 1 | 3 |
| 3 | 0 | 3 | 1 | 4 | 2 |
| 4 | 0 | 4 | 3 | 2 | 1 |

## Applications

- No integer congruent to 3 modulo 4 can be expressed as the sum of two squares.
- No integer congruent to 7 modulo 8 can be expressed as the sum of three squares.

  It transpires that any integer can be expressed as the sum of four squares, but this is harder to prove.
- $5 \mid (2^{3n+1} + 3^{n+1})$
- There is no integer solution to $\mathrm{x}^3 - \mathrm{x}^2 + \mathrm{x} + 1 = 0$.

- $641 \mid (2^{2^5} + 1)$.

## Solving congruences

The *residues modulo m* are $\mathbb{Z}_m = \{0, 1, 2, \dots (m–1)\}$.

Addition, subtraction and multiplication all work for residues, but what about division?

The *congruence* $ax \equiv c \pmod{m}$ has a solution for $x$ if, and only if, $(a, m) \mid c$.

**Proof:** Use Euclid's algorithm. The solution is unique modulo $m \div (a, m)$.

In particular, we can calculate the reciprocal of $a$ modulo $m$ if, and only if, $(a, m) = 1$. Such values $a$ are called *units* modulo $m$ and we write $\mathrm{U}_m = \{a \in \mathbb{Z}_m \mid a$ is a unit$\}$.

### Observation

- If $a, b \in \mathrm{U}_m$ then $ab \in \mathrm{U}_m$.

### Euler's totient function

Define $\varphi(m)$ to be the number of natural numbers less than $m$ and co-prime to $m$, so $\varphi(m)$ is the number of units modulo $m$.

Given a prime $p$, observe $\varphi(p) = (p - 1)$ and $\varphi(p^n) = p^n - p^{n-1}$.

## Wilson's theorem

If $p$ is a prime, then $(p–1)! \equiv -1 \pmod{p}$.

### Proof

Associate each of the numbers $1, 2, \dots$, p–1 with its reciprocal $(\bmod\, p)$. The reciprocal of $a$ may be the same as $a$, but only if $a^2 \equiv 1 \pmod{p}$ which requires $a = 1$ or $p–1$. Apart from these, the numbers $2, 3, \dots, p–2$ can be paired off so that the product of each pair is $1 \pmod{p}$. It follows that $2.3. \dots .(p–2) \equiv 1 \pmod{p}$. Multiply by $p–1 \equiv -1 \pmod{p}$ to obtain the result.

This proof actually fails if $p = 2$ or $3$, but these cases are easily verified independently.

## Chinese Remainder Theorem

Given two natural numbers $m$ and $n$ with greatest common divisor $1$, there is a simultaneous solution to the congruences $x \equiv a \pmod{m}$ and $x \equiv b \pmod{n}$ and this solution is unique $(\bmod\, mn)$.

### Proof

Use Euclid's algorithm to find $s$ and $t$ such that $ms + nt = 1$. Let $c = bms + ant$. Now $nt \equiv 1 \pmod{m}$ so $c \equiv ant \equiv a \pmod{m}$. Similarly $c \equiv b \pmod{n}$.

Suppose there is a further solution $d$. Observe that $c - d \equiv 0 \pmod{m}$ and $c - d \equiv 0 \pmod{n}$, so $c - d \equiv 0 \pmod{mn}$ as required.

### Corollaries

1. Euler's totient function is multiplicative: if $(m, n) = 1$ then $\varphi(mn) = \varphi(m)\varphi(n)$.

**Proof:** Given $c \in \mathrm{U}_m$ and $d \in \mathrm{U}_n$ find $e \in \mathbb{Z}_{mn}$ with $c \equiv e \pmod{m}$ and $d \equiv e \pmod{n}$. Then $e \in \mathrm{U}_{mn}$ and each such pair $(c, d)$ is linked to a unique $e$.

2. $\varphi(m) = m \prod_{\text{prime } p|m} (1 - {}^1\!/_p)$.

**Proof:** Consider the unique expression of $m$ as a product of primes.

## *Euler's theorem*[1]

Given $m \geq 2$ and $a$ with $(a, m) = 1$, then $a^{\varphi(m)} \equiv 1 \pmod{m}$.

### Proof

Let $\mathrm{U}_m = \{x \mid 0 < x < m \text{ and } (x, m) = 1\}$ be the set of units modulo $m$. Say $\mathrm{U}_m = \{u_1, u_2, \ldots u_f\}$ where $f = \varphi(m)$.

Multiply each of these $u_i$ by $a$ modulo $m$. The resulting values are coprime to $m$, since $u_i$ and $a$ are. Moreover they are distinct, since $a$ is a unit and can be divided, so $au_i = au_j \pmod{m} \Rightarrow u_i = u_j \pmod{m}$. So they are just a permutation of the $f$ values in $\mathrm{U}_m$.

Hence the product $(au_1)(au_2)\ldots(au_f) \equiv u_1u_2\ldots u_f \pmod{m}$. But $u_1, u_2, \ldots u_f$ are all units and so can be divided out, leaving $a^f \equiv 1 \pmod{m}$ as required.

### Corollary (Fermat's little theorem)[2]

Given a prime $p$ and $a$ not divisible by $p$, then $a^{p-1} \equiv 1 \pmod{p}$.

Moreover, for any $a$, $a^p \equiv a \pmod{p}$.

### Observation

This gives a test for primality. If a number $p$ does *not* satisfy $a^{p-1} \equiv 1 \pmod{p}$ for any single value of $a$, then $p$ can *not* be prime.

However, passing this test is not sufficient to prove primality. Composite numbers that satisfy the test are called *pseudo-prime* with respect to the base $a$. *Carmichael numbers*, such as $561$, are Fermat pseudo-primes for all possible bases $a$.

The Fermat-Euler test $a^{\frac{p-1}{2}} \equiv \pm 1 (\bmod p)$ is sharper but is still not sufficient. In particular, it reveals $561$ to be composite but fails to catch $1729$.

## *Public key cryptography*

With the increasing use of computer networks and digital, electronic communications, it becomes important to ensure that messages can be sent securely with the meaning revealed only to the intended recipient and that they can be authenticated as having been sent by the real originator.

The general approach is to choose some large modulus $m$ and encode blocks of a message as numbers in $\mathbb{Z}_m$.

[1] Humphreys & Prest, p 58.

[2] Humphreys & Prest, p 54.

Caesar's cypher encodes a message $a$ as $a + e \pmod{m}$ for some encryption key, $e$. This is decoded by calculating $(a + e) - e \equiv a \pmod{m}$. Unfortunately, the code is also easily broken by frequency analysis.

A further problem is the distribution of the keys. The key can be any secret shared by the two participants. How can one pass it safely to the other? The trick is to imagine a box with two locks and proceed as follows:

- The sender (conventionally called Alice) places the secret in the box, locks one of the locks with her key and sends the locked box to the recipient (conventionally called Bob).
- Bob locks the second lock with his key and returns the box to Alice.
- Alice unlocks the first lock and returns the box to Bob.
- Bob unlocks the second lock, opens the box and extracts the secret.

Note that Alice and Bob never have to share their private keys with anyone else but the box is always securely locked when in transit between them. The trick is to find an arithmetic equivalent of a box with two locks.

Modular addition is a possibility. Alice and Bob agree on a modular base $m$ (which can be made public) and choose private values $a$ and $b$. Alice now sends a shared secret $s$ to Bob as follows:

- A → B: $m_1 = s + a \pmod{m}$
- B → A: $m_2 = m_1 + b = s + a + b \pmod{m}$
- A → B: $m_3 = m_2 - \mathrm{a} = \mathrm{s} + b \pmod{m}$

Bob can now recover $s$. Unfortunately, anyone overhearing the conversation (traditionally called Eve) can recover $s = m_1 - m_2 + m_3$.

Modular multiplication is another possibility. As long as $a$ and $b$ are co-prime to $m$, Alice and Bob can calculate multiplicative inverses and replace the subtractions by divisions in the above protocol. The same problem arises and Eve can recover $s$ or, strictly speaking, $s \pmod{m/(m,s)}$ if $(m,s) > 1$.

However, modular exponentiation really does work.

## Diffie-Hellman key exchange[3]

Choose a large prime modulus, $p$. Pick $e$ with $(e, p{-}1) = 1$ and find $d$ such that $de \equiv 1 \pmod{p{-}1}$ so $de = 1 + (p{-}1)t$ for some $t$.

Then $(a^e)^d = a^{ed} = a^{1+(p-1)t} = a(a^{p-1})^t \equiv a1^t \pmod{p} = a$.

We now have a protocol:

- Alice chooses $p$ and the value $e$ and sends the message $a^e$ to Bob.
- Bob picks another value $f$ and sends $(a^e)^f$ back to Alice.
- Alice works out $((a^e)^f)^d = ((a^e)^d)^f = a^f$ and sends it back to Bob.
- Bob now decodes this similarly to find $a$.

Breaking this requires *discrete logarithms*, which is as hard as factoring a large integer.

[3] Davenport, p 191.

## The RSA code[4]

The Rivest, Shamir and Adleman (RSA) public key system[5] uses Euler's Theorem to provide secure communications and digital signatures.

Let $p$ and $q$ be two primes with product $m$ so $\varphi(m) = (p–1)(q–1)$. Choose $e$ (the *encryption exponent*) relatively prime to $\varphi(m)$ and use Euclid's algorithm to find $d$ (the *decryption exponent*) and $c$ such that $ed + \varphi(m)c = 1$ so $ed \equiv 1 \pmod{\varphi(m)}$.

Now, given $a < p, q$, $(a^e)^d = a^{ed} = a^{1-\varphi(m)c} = a(a^{\varphi(m)})^{-c} \equiv a1^{-c} = a \pmod m$ provided $(a, m) = 1$, which is ensured by $a < p, q$.

We now have a protocol:

- Alice picks two large primes and publishes their product $m$ and the value $e$.
- Bob encodes a message $a$ as $a^e \pmod m$ and sends it to Alice.
- Alice recovers $a$ by raising the encoded message to the power $d \pmod m$.

Anyone intercepting the message knows $m$ and $e$ but not $d$ which can only be calculated easily if $\varphi(m)$ is known. However, this is believed to be difficult, at least as difficult as factoring $m$.

Conversely, if $d$ is known, then $m$ can be factored as follows:

$de \equiv 1 \pmod{\varphi(m)}$, so suppose that $de - 1 = n\varphi(m)$. Observe $\varphi(m) = (p–1)(q–1) = pq - p - q + 1$, which is slightly smaller than $pq = m$. So $n$ is slightly greater than $(de - 1)/m$. Calculating this fraction and rounding up will give $n$.

Once $n$ is known, $\varphi(m) = (de - 1)/n$. Now $m + 1 - \varphi(m) = p + q$ and $m = pq$, so $p$ and $q$ are the roots of the quadratic equation $x^2 - (m + 1 - \varphi(m))x + m = 0$.

The encoding and decoding processes are symmetric and can be performed in either order. Thus Alice can prove her identity by taking a challenge $a$ and returning $a^d \pmod m$ which anyone can then decode but only she could have encoded.

## Coin-tossing by telephone[6]

Let $p$ be a prime of the form $4k+3$ and suppose $a \equiv x^2 \pmod p$. Now $x^{4k+2} = x^{p-1} \equiv 1 \pmod p$, so $(a^{k+1})^2 \equiv x^{4k+4} \equiv x^2 \equiv a \pmod p$ and $x = a^{k+1}$ is a solution to the original equation. So we can calculate square roots $\bmod p$.

Let $p$ and $q$ be two such primes with product $n$ and suppose $a \equiv z^2 \pmod n$. Now $a$ is also a square modulo both $p$ and $q$, say $a \equiv x^2 \pmod p$ and $a \equiv y^2 \pmod q$. Use the Chinese Remainder Theorem to construct 4 solutions $z \equiv \pm s, \pm t \pmod n$.

Observe that, if we know both $s$ and $t$, it is possible to factor $n$. $s^2 \equiv t^2 \equiv a \pmod n$, so $pq = n | (s^2 - t^2) = (s+t)(s-t)$. However, $s$ and $t$ are distinct so neither $(s+t)$ nor $(s-t)$ is divisible by $n$. Without loss of generality, $p|(s+t)$ and $q|(s-t)$, and we can use Euclid to find $p$ and $q$ as the HCFs of $n$ and $(s+t)$ and $(s-t)$ respectively.

We now have a protocol:

- Alice picks two large primes and tells Bob their product $n$.

[4] Humphreys & Prest, p 60.

[5] R Rivest, A Shamir & L Adleman: *A method for obtaining digital signatures and public-key cryptosystems,* Communications ACM 21(2), February 1978, pp 120-6.

[6] Giblin, p 145.

- Bob picks $s$ co-prime to $n$ and tells Alice $a \equiv s^2 (\operatorname{mod} n)$.
- Alice calculates the 4 roots, picks one at random and tells Bob.
- If this is $\pm s$, Bob concedes defeat. Otherwise it is $\pm t$ which allows Bob to factor $n$ and, by so doing, win.

### Practical remarks

These mathematical results are not sufficient by themselves to build secure encryption systems. Care must be taken over the actual choice of the prime numbers used and, even more importantly, over the systems procedures. The security course explores these issues further.

## *Exercises*

1. Show that a number is divisible by $9$ if, and only if, the sum of its digits is divisible by $9$. (This is known as *casting out the 9s*.) For example, $23714$ is not divisible by $9$ as $2+3+7+1+4 = 17$ which is not divisible by $9$.
2. Find a similar test for divisibility by $11$.
3. Is it possible to form a sum of numbers using each of the digits $0$ to $9$ exactly once whose total is $100$? (Tricks like exponentiation are not allowed.)
4. A $1\ 000\ 000$ digit number is exactly divisible by $99$. A new number is formed by reversing the order of its digits. What is the probability that the new number is also exactly divisible by $99$?
5. The International Standard Book Number (ISBN) found in the front of many books is a 10 digit code such as 0-521-35938-4 (where the hyphens can be ignored). In this case, the 0 indicates that the book was published in the UK and some other English speaking countries, 521 is the publisher (the Cambridge University Press), 35938 is the book number and 4 a check digit. The check digit is chosen so that if the ISBN is $d_1 d_2 \ldots d_{10}$ then $d_{10} = \sum_{i=1}^{9} i \cdot d_i (\operatorname{mod} 11)$. It may be that the last digit has to be 10, in which case X is written, as in 0-387-97993-X.

   Prove that $\sum_{i=1}^{10} i \cdot d_i \equiv 0 (\operatorname{mod} 11)$ and verify that the two given ISBNs satisfy the congruence. Prove that the check digit will show up common copying errors caused by interchanging two adjacent digits (so, for example, 67 becomes 76) or doubling the wrong one of a triple (so, for example, 667 becomes 677). Why do you think the modulus 11 was chosen instead of the more natural 10?
6. Show that the equation $x^5 - 3x^2 + 2x - 1 = 0$ has no solutions for $x \in \mathbb{Z}$.
7. Solve the following congruences:
   - $77x \equiv 11 \ (\text{mod } 40)$
   - $12y \equiv 30 \ (\text{mod } 54)$
   - $z \equiv 13 \ (\text{mod } 21)$ and $3z \equiv 2 \ (\text{mod } 17)$
8. A band of 15 pirates acquires a hoard of gold pieces. When they come to divide up the coins, they find that three are left over. Their discussion of what to do with these extra coins becomes animated and, by the time some semblance of order returns, there remain only seven pirates capable of making an effective claim on the hoard. However, when the hoard is divided between these seven, it is found that two pieces are left over. There ensues an unfortunate repetition of the earlier disagreement, but this does at least have the consequence that the four pirates who remain are able to divide the hoard evenly

between themselves. What is the smallest number of gold pieces that could have been in the hoard?[7]

9. Calculate $20!\ 21^{20} \pmod{23}$.

10. Calculate $3^{1000000000} \pmod{257}$.

11. Show that $42 \mid n^7 - n$ for all positive integers $n$.

12. An unwise person publishes the RSA enciphering scheme $(m, e) = (3901, 1997)$ via which he wishes to receive messages. You intercept the transmission

    1099 1307 2477 3490 0506 0615 0952 2697 0016 3333 0601

    Factor $m$ and hence find the deciphering key $d$ such that $de \equiv 1 \pmod{\varphi(m)}$. Assuming that each block of four digits encodes two letters under the map a-z, space, ?, !, 0-9 become 00-25, 26, 27, 28, 29-38, decipher the text.

13. The previous question uses code blocks that are larger than the two primes whose product forms the base. Verify that a particular code block which shares a factor with $m$ still can be encoded and decoded correctly. Why does this work?

14. $11$ is a prime of the form $4k + 3$ (with $k = 2$) so we can extract the square root of $a$ by raising $a$ to the power $k + 1 = 3$. For example, the square root of $5$ is $5^3 = 125 \equiv 4 \pmod{11}$ and we can check that $4^2 = 16 \equiv 5 \pmod{11}$. However, the same approach fails to calculate the square root of $6$. Explain.

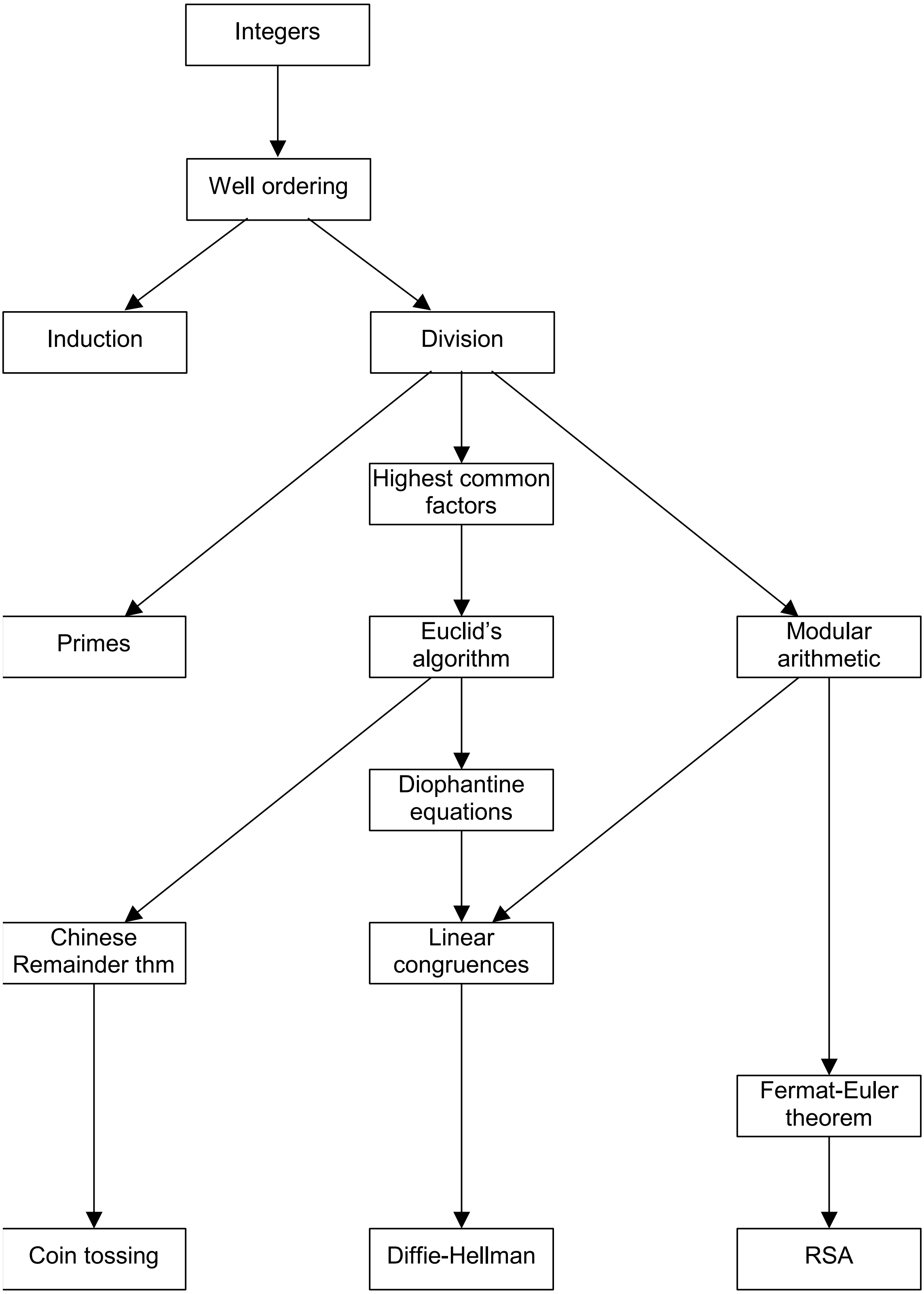
15. Write an ML function to calculate the reciprocal of a number to a given modular base. This may well use the function for Euclid's algorithm written earlier.

16. Write an ML function to calculate powers of numbers to a given modular base.

[7] Humphreys & Prest, p 50.

# Revision guide

The following diagram shows the development of the key ideas presented in the first half of the course:



# Lecture review form

If high lecturing standards are to be maintained and lower standards to be raised, it is important for lecturers to receive feedback about their lectures. Consequently, we would be grateful if you would complete this questionnaire and return it to the Student Administration Office. A digest of the information will be passed to the Staff-Student Liaison and Teaching Committees.

## *Discrete Mathematics (Part A)*<br>*Michaelmas 2001*

Please tick the boxes below:

### Interest

| | | | |
|---|---|---|---|
| Tedious | Uninteresting | Interesting | Exciting |

### Level of material

| | | | | | | |
|---|---|---|---|---|---|---|
| Much too basic | Too basic | Slightly basic | About right | Slightly complicated | Too complicated | Much too complicated |

### Breadth of coverage

| | | | | | | |
|---|---|---|---|---|---|---|
| Much too general | Too general | Slightly general | About right | Slightly specific | Too specific | Much too specific |

### Organisation of lectures

| | | | |
|---|---|---|---|
| Chaotic | Confused | Adequate | Brilliant |

### Assumptions

| | | |
|---|---|---|
| Assumed too little | About right | Assumed too much |

### Ease of understanding

| | | | |
|---|---|---|---|
| Incomprehensible | Confused | Adequate | Clear |

### Speed

| | | | | | | |
|---|---|---|---|---|---|---|
| Much too slow | Too slow | Slightly slow | About right | Slightly fast | Too fast | Much too fast |

### Delivery

| | | | |
|---|---|---|---|
| Incoherent | Halting | Adequate | Fluent |

### Notes

| | | |
|---|---|---|
| Poor | Adequate | Excellent |

### Supervision

| | | |
|---|---|---|
| Poor | Adequate | Excellent |

PTO

### Best thing about the course

### Worst thing about the course

### Further comments