

## Numbers Revisited

$\mathbb{E}$  = Natural Numbers,  $\{0,1,2,\dots\}$ .  $\mathbb{Z}$  (Or  $\mathbb{I}$ ) = The Integers,  $\{\dots,-2,-1,0,1,2,\dots\}$ .  
Shorthand: If  $A$  is a set, “ $a \in A$ ” means the following: ‘ $a$  is an element of  $A$ ’. If  $A$  and  $B$  are sets, “ $A \subseteq B$ ” means ‘ $A$  is a subset of  $B$ ’. This is interpreted as “if  $a \in A$ , then  $a \in B$ ”.

Primes as the building blocks of numbers. Definition: A positive integer  $p$  is prime if it has exactly two positive divisors, namely 1 and  $p$ . *Understanding* the definition. As we expect, 2, 3, 5, 7, etc., are primes. But 1, 0, 4, etc., are not — 1 has exactly one divisor; 0 is not a +ve integer;  $4 = 2 \times 2$  as well as  $1 \times 4$  (3 divisors); etc.

What **exactly** is a divisor? Given integers  $a$  and  $b$ , we say that  $a$  divides  $b$  (written  $a|b$ ) if there is some *integer*  $k$  so that  $ak = b$ . So, for instance,  $-2|2$  because  $(-2)(-1) = 2$ . (here  $k = -1$ ). We “know” that (1) there are **infinitely** many prime numbers; (2) any number **greater** than 1 can be written as a product of primes. Why are these facts true? The secret is to *understand* division.

Theorem (The **Division** Algorithm, page 10). If  $a, b \in \mathbb{E}$  with  $a > 0$ , then there are natural numbers  $q, r \in \mathbb{E}$  with  $0 \leq r < a$  such that  $b = qa + r$  ( $q$  is the **quotient**,  $r$  is the **remainder**). Examples:  $a = 6, b = 16$  so  $q = 2, r = 4$ . Reverse the roles of  $a$  &  $b$ :  $a = 16, b = 6$  so  $q = 0, r = 6 = b < 16$ . If  $a|b$  then  $r = 0$  and conversely. Thus  $6|18$  and  $a = 6; b = 18$  gives  $q = 3, r = 0$ .

### Greatest Common Divisor (gcd)

Given  $m, n \in \mathbb{Z}$ , with  $m, n \neq 0$ , a **positive** integer  $d \in \mathbb{Z}$  is called a **gcd** of  $m$  and  $n$  if (1)  $d|m$  and  $d|n$  (common divisor); (2) If  $t|m$  and  $t|n$ , then  $t|d$ . *Refer* to the book for the proof that gcd’s always exist and are unique. How to calculate gcd’s: use **Euclid’s Algorithm**. It inputs two numbers  $a$  &  $b$  and outputs their gcd in the form  $as + bt$  for some  $s, t \in \mathbb{Z}$ .

**Example:** Find  $d = \gcd(92, 394)$  in the form  $92s + 394t$ . A:  $394 = 4 \times 92 + 26$  (By the division algorithm). Commentary: If  $d|394$  and  $d|92$ , then  $d|26$ . On the other hand, if  $t|26$  and  $t|92$ , then  $t|394$ . Hence  $\gcd(26, 92) | \gcd(92, 394)$  and vice versa. The 2 gcd’s are equal. Repeat with 92, 26:  $92 = 3 \times 26 + 14$ . Thus  $d = \gcd(14, 26)$ . Repeat again:  $26 = 1 \times 14 + 12$ . Thus  $d = \gcd(12, 14)$ . Repeat:  $14 = 1 \times 12 + 2$ . Thus  $d = \gcd(2, 12)$ . Repeat:  $12 = 6 \times 2 + 0$ . We have a zero remainder so  $d = \gcd(92, 394) = 2$  (The Remainder of the line “above”).

We now **need** to express ‘2’ in the form  $92s + 394t$ . From (iv) on the right,  $2 = 14 - (1 \times 12)$ .  $2 = 14 - (26 - 14)$  from step (iii).  $2 = 2 \times 14 - 16$ .  $2 = 2(92 - 3(26)) - 16$  from step (ii).  $2 = 2 \times 92 - 7 \times 26$ .  $2 = 2 \times 92 - 7(394 - 4(92))$  from step (i).  $2 = 30 \times 92 - 7 \times 394$ . This is the **desired** form, so  $s = 30$  and  $t = -7$ .

#### **Recap:**

- (i)  $394 = 4 \times 92 + 26$
- (ii)  $92 = 3 \times 26 + 14$
- (iii)  $26 = 1 \times 14 + 12$
- (iv)  $14 = 1 \times 12 + 2$
- (v)  $12 = 6 \times 2 + 0$ .

Note: Although the *algorithm* outputs a suitable  $s$  and  $t$ , so that  $d = as + bt$ , there are **infinitely** many ways of solving for  $s$  and  $t$  as the equation does not uniquely determine  $s$  and  $t$ . For example,  $2 = \gcd(4, 6) = 1 \times 6 - 1 \times 4$ . But also  $5 \times 6 - 7 \times 4 = 2$ . Here,  $(1+4) \times 6 - (1+6) \times 4 = 2$ ;  $(1 \times 6) - (1 \times 4) + (4 \times 6) - (4 \times 6) = 2$ . In general,  $as + bt = d$ ;  $a(s + kb) + b(t - ka) = d$ .

## Tutorial

Show **that** if  $\gcd(a,c) = 1 = \gcd(b,c)$ , then  $\gcd(ab,c) = 1$ . A: **Suppose**  $ar+cs = 1$  (1). Then if  $d|a$  and  $d|c$ , then  $d|1$  so that  $d = 1$  or  $-1$ . Thus  $\gcd(a,c) = 1$ . (we'll *need* this later). Now suppose that  $\gcd(a,c) = 1$ , so there are  $r,s \in \mathbb{Z}$  **satisfying**  $ar+cs = 1$ . Similarly, there are  $r',s' \in \mathbb{Z}$  such that  $br'+cs' = 1$ . Multiply (1) by  $br'$ :  $ab(rr')+c(br's) = br'$ . **Add**  $cs'$ :  $ab(rr')+c(br's+s') = br'+cs' = 1$ . So  $\gcd(ab,c) = 1$ .

Q: Let  $p_1 = 2, p_2 = 3, \dots$  be the list of primes arranged in increasing order. Consider products of the form  $(p_1 \times \dots \times p_n) + 1$ . Show that this number is prime if  $n = 1$  to  $5$ ; but that it is **not** prime for  $n = 6$ . What prime factors does it have? A: The numbers are 3, 7, 31, 211, 2311. The next is 30031 *which* is  $59 \times 509$ .

Q: Show that if  $2^n - 1$  is prime, then  $n$  must be prime. A: **Suppose** that  $2^n - 1$  was prime but  $n = rs$ . Then  $2^n - 1 = (2^r)^s - 1 = (2^r - 1)(1 + 2^r + \dots + 2^{r(s-1)})$  [Using the G.P. formula  $1 + x + x^2 + \dots + x^t = (x^{t+1} - 1)/(x - 1)$ ]. As  $2^n - 1$  is prime, then  $2^r - 1$  must be 1, so  $r = 1$  and  $n$  **must** therefore be prime.

**Important** idea: 2 integers  $a, b$  are coprime if  $\gcd(a, b) = 1$ . Examples: (i) *Distinct* primes are coprime. (ii) 6 and 25 are coprime. (iii)  $n$  and  $n+1$  are *always* coprime. Application: Given a fraction  $r/s$ , there's an equivalent fraction  $r'/s'$  with  $r'$  and  $s'$  **coprime**. Intuitively, *equivalent* means  $r/s$  and  $r'/s'$  represents the same number. But **this** is a bit vague! We say  $r/s$  is equivalent to  $u/v$ ,  $r/s \sim u/v$ , if  $rv = us$ . For example,  $1/2 \sim 2/4$  since  $1 \times 4 = 2 \times 2$ . [ $r/s \sim r'/s'$  since  $rst = rst$ ].

8th February 1999

**Proof** of this obvious fact: Let  $d = \gcd(r, s)$ . Then  $d|r$  so there is *some*  $r' \in \mathbb{Z}$  such that  $r = r'd$ . Similarly,  $d|s$  so there is an  $s' \in \mathbb{Z}$  with  $s = s'd$ . So we *have*  $rs' = r'ds' = r's'd = r's$ . We still need to check that  $\gcd(r', s') = 1$ . We know that  $d = \alpha r + \beta s$  for some  $\alpha, \beta \in \mathbb{Z}$ . Also,  $d = \alpha r'd + \beta s'd = d(\alpha r' + \beta s')$ . **Thus**  $1 = \alpha r' + \beta s'$ .

**Note:** if  $\alpha = \alpha x \in \mathbb{Z}$ , then  $\alpha - \alpha x = 0$ ,  $\alpha(1-x) = 0$ . In  $\mathbb{Z}$ , we don't get two non-zero numbers whose product is *zero*. Because  $\alpha$  is not 0, then  $(1-x) = 0$ , thus  $x = 1$ . Note: given any *expression* of this form, then  $\gcd(r', s') = 1$  **since** if  $t|r'$  and  $t|s'$ , then  $t|1$ . So if  $t > 0$ ,  $t = 1$ .

**Proposition:** If  $a, b, c$  are +ve integers, with  $a, b$  coprime, then (i) if  $a|bc$  **then**  $a|c$ , (ii) if  $a|c$  and  $b|c$  **then**  $ab|c$ . **Proof:** As  $a$  and  $b$  are coprime, there are  $r, s \in \mathbb{Z}$  with  $ar+bs = 1$ , and so  $arc+bsc = c$ . (i) if  $a|bc$ , it divides the *second* term,  $bsc$ , and hence also the sum i.e.  $a|c$ . (ii) If  $a|c$ ,  $c = au$  for some  $u$ . If  $b|c$ , then  $c = bv$  for **some**  $v$ , and hence  $arbv+bsau = c$ ,  $abr+absu = c$ ,  $ab(rv+su) = c$  *and*  $ab|c$ .

**Corollary.** If  $p|ab$ , with  $a, b \in \mathbb{Z}$ , and  $p$  is *prime*, then  $p|a$  or  $p|b$ . Proof: If  $p|a$  then **fine**, we're done! If it doesn't, then  $p$  and  $a$  are *coprime*. Apply (i) of the proposition to get  $p|b$ .

## Tutorial: Alternative Matrix Method for Calculating gcd's

To find  $\gcd(a,b) = d$  in the form  $ar+bs$ , set up this **partitioned** matrix:  $\begin{pmatrix} 1 & 0 & | & b \\ 0 & 1 & | & a \end{pmatrix}$ . Set  $b = aq_1+r_1$  with  $0 \leq r_1 \leq a$ . If  $r_1 = 0$ , then **STOP**, and  $a = \gcd(a,b)$ . If  $r_1 \neq 0$ , *subtract*  $q_1$  times the bottom row from the top row, to get the matrix  $\begin{pmatrix} 1 & -q_1 & | & r_1 \\ 0 & 1 & | & a \end{pmatrix}$ . Now write  $a = r_1q_2 + r_2$  with  $0 \leq r_2 \leq r_1$ . If  $r_2 = 0$ , then **STOP**. If  $r_2 \neq 0$ , continue, but now operating on the second row, until **eventually** we get some  $r_k = 0$ .

Example:  $\gcd(171, 30) = \begin{pmatrix} 1 & 0 & | & 171 \\ 0 & 1 & | & 30 \end{pmatrix} \sim \begin{pmatrix} 1 & -5 & | & 21 \\ 0 & 1 & | & 30 \end{pmatrix} \sim \begin{pmatrix} 1 & -5 & | & 21 \\ 0 & 1 & | & 9 \end{pmatrix} \sim \begin{pmatrix} 3 & -1 & | & 3 \\ 0 & 1 & | & 9 \end{pmatrix} \sim \begin{pmatrix} 3 & -10 & | & -57 \\ 0 & 1 & | & 9 \end{pmatrix}$ . So  $\gcd(171, 30) = 3 = 3 \times 171 - 17 \times 30$ . **Note:** any row  $(u \ v \ | \ w)$  represents  $bu+av = w$ .  
 Example:  $\gcd(91, 126) = \begin{pmatrix} 1 & 0 & | & 126 \\ 0 & 1 & | & 91 \end{pmatrix} \sim \begin{pmatrix} 1 & -1 & | & 35 \\ 0 & 1 & | & 91 \end{pmatrix} \sim \begin{pmatrix} 1 & -2 & | & 35 \\ 0 & 1 & | & 21 \end{pmatrix} \sim \begin{pmatrix} 3 & -2 & | & 14 \\ 0 & 1 & | & 21 \end{pmatrix} \sim \begin{pmatrix} 3 & -5 & | & 7 \\ 0 & 1 & | & 21 \end{pmatrix} \sim \begin{pmatrix} 13 & -5 & | & 0 \\ 0 & 1 & | & 7 \end{pmatrix}$ . So  $\gcd(126,91) = 7 = -5 \times 126 + 7 \times 91$ .

Q: Let  $a_1, \dots, a_n$  be +ve integers. Their **greatest common divisor**,  $\gcd(a_1, \dots, a_n)$ , is the +ve integer  $m$  such that  $m|a_i$  for each  $i$ , and *whenever*  $c$  is an integer with  $c|a_i$  for each  $i$ , then  $c|m$ . Q: Show that  $\gcd(a_1, a_2, a_3) = \gcd(a_1, \gcd(a_2, a_3))$  and so **find**  $\gcd(356, 249, 145)$ . Can it be *written* in the form  $r_1 \times 356 + r_2 \times 249 + r_3 \times 145$ ?

A: Let  $d_1 = \gcd(a_1, \gcd(a_2, a_3))$ . **Then**  $d_1|a_1$  and  $d_1|\gcd(a_2, a_3)$ , so that  $d_1|a_2$  and  $d_1|a_3$ . *Writing*  $d_2 = \gcd(a_1, a_2, a_3)$ , we have by **definition that**  $d_1|d_2$ . Now  $d_2|a_1$  and  $d_2|a_2$  and  $d_2|a_3$ . *Looking at the last two of these, we get*  $d_2|\gcd(a_2, a_3)$ . (By the *definition* of the gcd's once again). So we **know** that  $d_2|a_1$  and  $d_2|\gcd(a_2, a_3)$ , but this **must mean that**  $d_2$  *must divide*  $d_1$ . We thus have  $d_1|d_2$  and  $d_2|d_1$ , and so because both are *positive*, we must have  $d_1 = d_2$ . This gives us a way of **calculating**  $\gcd(356, 249, 145)$  in the usual method giving  $\gcd(249, 145) = 1 = -46 \times 249 + 79 \times 145$ . At this stage, we see that  $\gcd(356, 249, 145) = 1$  *since 1 divides 356* (cunning!) and we have  $1 = -46 \times 249 + 79 \times 145 + 0 \times 356$ , completing the answer to the question.

Q: Can this be done in **general** i.e. is  $\gcd(a_1, \dots, a_n) = \sum_{i=1}^n r_i a_i$ ? A: We can **clearly** do this for  $n = 2$ . **Suppose** we can do it for  $a_1, \dots, a_{n-1}$  so that  $d = \gcd(a_1, \dots, a_{n-1}) = \sum s_i a_i$ , say. Now  $\gcd(a_1, \dots, a_n) = \gcd(\gcd(a_1, \dots, a_{n-1}), a_n)$  by the *same sort of argument as above* (case  $n = 2$ ).  $\gcd(a_1, \dots, a_n) = rd_1 + sa_n$  ( $sa_n = \gcd(d_1, \dots, a_n)$ ) =  $r \sum_{i=1}^{n-1} (s_i a_i + sa_n) = \sum_{i=1}^{n-1} (rs_i) a_i + sa_n$ , which has the **correct** form i.e.  $\sum_{i=1}^n r_i a_i$ .

Q: The **least common multiple** of  $a_1, \dots, a_n$  is the unique +ve integer  $m$  s.t.  $a_i|m$  for each  $i$ , and **whenever**  $c$  is an integer with  $a_i|c$  for each  $i$ , then  $m|c$ . (i) *Show that*  $\text{lcm}(a_1, a_2, a_3) = \text{lcm}(a_1, \text{lcm}(a_2, a_3))$ . (ii) **Find**  $\text{lcm}(123, 456)$ . (iii) Find a *formula linking*  $\text{lcm}(a_1, a_2)$  with  $\gcd(a_1, a_2)$ .

A: (i) **Compare** with the above. Let  $m_1 = \text{lcm}(a_2, a_3)$ , and then set  $m_1 = \text{lcm}(a_1, m_1)$ . **Then**  $a_1|m_1$  and  $m_1|m_1$ , so  $a_2|m_1$  and  $a_3|m_1$ , i.e. **writing**  $m_2 = \text{lcm}(a_1, a_2, a_3)$ , we get  $m_2|m_1$ . Now  $a_2|m_2$  and  $a_3|m_2$ , so  $m_1|m_2$ . Also,  $a_1|m_2$  so  $m_1|m_2$  and  $m_1 = m_2$ . (ii)  $\begin{pmatrix} 1 & 0 & | & 456 \\ 0 & 1 & | & 123 \end{pmatrix} \sim \begin{pmatrix} 1 & -3 & | & 87 \\ 0 & 1 & | & 123 \end{pmatrix} \sim \begin{pmatrix} 1 & -3 & | & 87 \\ 0 & 1 & | & 36 \end{pmatrix} \sim \begin{pmatrix} 3 & -1 & | & 15 \\ 0 & 1 & | & 36 \end{pmatrix} \sim \begin{pmatrix} 3 & -7 & | & 15 \\ 0 & 1 & | & 6 \end{pmatrix} \sim \begin{pmatrix} 17 & -7 & | & 3 \\ 0 & 1 & | & 6 \end{pmatrix} \sim \begin{pmatrix} 17 & -41 & | & 3 \\ 0 & 1 & | & 0 \end{pmatrix}$ . So  $\gcd(123, 456) = 3 = 17 \times 456 - 63 \times 123$ . **But**,  $-41 \times 456 + 152 \times 123 = 0$ , so  $152 \times 123 = 41 \times 456 = 18696$ . So 18696 is a *common multiple* of 123 and 456. Is it the lcm? Note:  $152 = 456/3$  and  $41 = 123/3$ . To **verify** that this is the lcm, we turn to 3(iii).

Let  $d = \gcd(a_1, a_2)$ , then  $a_1 = da'_1$  and  $a_2 = da'_2$ . Clearly,  $da'_1a'_2$  is a *common multiple* of  $a_1$  and  $a_2$  — but is it the **lcm**? Set  $m = \text{lcm}(a_1, a_2)$ , then  $m|da'_1a'_2$ . Claim:  $m = da'_1a'_2 = a_1a_2/d$ , i.e.  **$\text{lcm}(a_1, a_2) = a_1a_2/\gcd(a_1, a_2)$** . **Proof** of claim: suppose that  $a_1|c$  (so  $c = a_1b_1$  for some  $b_1$ ) and  $a_2|c$ , giving  $c = a_2b_2$ . Then  $a'_1db_1 = a'_2db_2$ . As  $d \neq 0$ ,  $a'_1b_1 = a'_2b_2$ . **BUT**,  $a'_1$  and  $a'_2$  are *coprime*, so as  $a'_1|a'_2b_2$  and  $a'_1|b_2$  (by the **lemma** we proved), then  $b_2 = a'_1b'_2$  for some  $b'_2$ .

We **thus** have  $c = a_2a'_1b'_2 = (da'_1a'_2)b'_2$  so that  $da'_1a'_2|c$ . **Thus**  $da'_1a'_2$  is the lcm as claimed. Note: as we *reduce*  $\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \begin{matrix} a_1 \\ a_2 \end{matrix}$  to  $\begin{pmatrix} r & s \\ -s' & r' \end{pmatrix} \begin{matrix} d \\ 0 \end{matrix}$ , the matrix *will always have determinant 1*, so that  $rs' - r's = 1$ . We therefore **know that**  $ra_1 + sa_2 = d$  (1) and  $r'a_1 + s'a_2 = 0$  (2). Using (2), **substitute** for  $a_1$  in terms of  $a_2$ :  $r(-s'a_2/r') + sa_2 = d$ . **Multiply** through by  $r'$  and sort out the resulting expression a bit:  $a_2(r's - rs') = r'd$ , but  $r's - rs' = -1$  (it is the negation of the determinant of the *matrix*) so  $-r' = a_2/d$  and  $-r'a_1 = a_1a_2/d = s'a_2$  as we *thought*.

Q: **Find**  $\gcd(30, 42, 70, 135)$ . A:  $\gcd(30, 42) = 6$ ,  $\gcd(6, 70) = 2$ ,  $\gcd(2, 135) = 1$ , so  $\gcd(30, 42, 70, 135) = 1$ .

12th February 1999

## Generalisation

**Corollary.** If  $p$  is prime, and  $p|a_1 \times \dots \times a_n$ , with all  $a_i$  being integers, then **there** is an  $i$ ,  $1 \leq i \leq n$ , such that  $p|a_i$ . Proof: if  $n = 1$ , there is *nothing* to prove. Suppose that we know the result of all products of  $(n-1)$  numbers or fewer. **Suppose further that**  $p|a_1 \times \dots \times a_n$ . But  $a_1 \times \dots \times a_n = (a_1 \times \dots \times a_{n-1})a_n$ . So  $p|a_1 \times \dots \times a_{n-1}$ , or  $p|a_n$  (by the **previous** result). If  $p|a_n$ , yippee! *Otherwise*,  $p|a_1 \times \dots \times a_{n-1}$ . But we know the result for any product of  $(n-1)$  numbers, so there's an  $i$ ,  $1 \leq i \leq a_{n-1}$ , with  $p|a_i$ . QED.

**Theorem.**  $\sqrt{2}$  is an irrational number. (so it cannot be *written as a ratio of 2* whole numbers). Proof: Suppose that  $\sqrt{2}$  is rational, so there is a **fraction**  $r/s$ , with  $\sqrt{2} = r/s$ . We will **assume** that  $r/s$  is in its lowest form i.e.  $\gcd(r, s) = 1$ . *Squaring* both sides gives  $2 = r^2/s^2$ . So  $2s^2 = r^2$  (\*). **Thus**  $2|r^2$ . But if  $2|r^2$  then also  $2|r$  by an *earlier* result. As  $2|r$ , then  $r = 2r'$  for **some**  $r'$ .  $2s^2 = 4(r')^2$ ;  $2r'^2 = s^2$ . So  $2|s^2$ , meaning that  $2|s$ . As  $\gcd(r, s) = 1$ , we cannot have  $2|r$  and  $2|s$ , so the *assumption that*  $\sqrt{2} = r/s$  is not true. This is a **form** of a proof to show that the expressions  $\sqrt{p}$  and  $\sqrt{(pq)}$  are irrational. ( $p$  &  $q$  being prime numbers).

## Prime Factorisation Theorem

Every **+ve integer n** greater than 1 may be written as a *product* of prime numbers,  $n = p_1 \times \dots \times p_r$ . This *prime factorisation* is unique, except in the order in which the factors appear. Explanation:  $354 = 2 \times 177 = 2 \times 3 \times 59$ . If  $n$  is not prime, then  $n = ab$ , with  $1 < a, b < n$ . We form tree diagrams for these, with **possible** prime factorisations for each branch. Put these together *to get a factorisation for n*.

*Theorem (Euclid):* there are *infinitely* many prime numbers. Proof: if there were only **finitely** many primes, we could list them all:  $p_1, p_2, \dots, p_n$ . Now look at  $N = (p_1 \times \dots \times p_n) + 1$ . This number has a *prime decomposition*, so there is a prime  $p$  that divides  $N$ . But this prime is not on our list, because for any *listed* prime  $p_i$ ,  $N$  gives remainder 1 on *division* by  $p$  (i.e.  $p_i \nmid N$ ).

## Section 2: Algebraic Identities

### The Binomial Theorem

$(a+b)^n = a^n + na^{n-1}b + \dots + \binom{n}{r}a^{n-r}b^r + \dots + b^n$ . Why does this *work*? A simple explanation (not a formal proof):  $(a+b)^n = (a+b)(a+b)\dots(a+b)$  [n times]. **Multiplying** this out, we get lots of terms in  $a^{n-r}b^r$ . Each term is obtained by *picking out r brackets* from which we take b. For example, in  $(a+b)(a+b)(a+b)(a+b)(a+b)(a+b)(a+b)(a+b)(a+b)$ , the red brackets indicate that we multiply *with a b*, and in the others we multiply with an a, hence we get  $a^5b^4$ . We can do this (pick out r brackets from n brackets) in  $\binom{n}{r}$  different ways, so the **coefficient** of  $a^{n-r}b^r$  is  $\binom{n}{r}$ . Note:  $\binom{n}{r} = \frac{n!}{(n-r)!r!}$ .

To **prove** this result, we use Proof By Induction. Plan: **Check** the result for  $n = 1$  i.e.  $(a+b)^1 = a^1+b^1 = a^1b^0+a^0b^1 = \sum_{r=0}^1 \binom{1}{r}a^{1-r}b^r$ . (**Check** that  $\binom{1}{1} = 1$ ,  $\binom{1}{0} = 1$ ). [NOTES: *Exploration*.  $(a+b)^2 = a^2+ab$  (from  $a(a+b)$ ) +  $ab+b^2$  (from  $b(a+b)$ ) =  $a^2+2ab+b^2$ . And  $(a+b)^3 = a^3+2a^2b+ab^2$  [from  $a(a^2+2ab+b^2)$ ] +  $a^2b+2ab^2+b^3$  [from  $b(a^2+2ab+b^2)$ ] =  $a^3+3a^2b+3ab^2+b^3$ ].

Next we **assume** that we have the *formula*  $(a+b)^n = \sum_{r=0}^n \binom{n}{r}a^{n-r}b^r$  for some n, and we look at  $(a+b)^{n+1}$ . *But*,  $(a+b)^{n+1} = (a+b)(a+b)^n = (a+b)(\sum_{r=0}^n \binom{n}{r}a^{n-r}b^r) = \sum_{r=0}^n \binom{n}{r}a^{n+1-r}b^r + \sum_{r=0}^n \binom{n}{r}a^{n-r}b^{r+1} = \sum_{r=0}^n \binom{n}{r}a^{(n+1)-r}b^r + \sum_{s=1}^{n+1} \binom{n}{s-1}a^{(n+1)-s}b^s$  [the **last part** writes s for r+1] =  $\sum_{s=0}^{n+1} \{ \binom{n}{s-1} + \binom{n}{s} \} a^{n+1-s}b^s$ . We now **want to show that**  $\binom{n}{s-1} + \binom{n}{s} = \binom{n+1}{s}$ . This is a *lemma* we must prove.

**Proof:**  $\binom{n}{s-1} = \frac{n!}{(n-s+1)!(s-1)!}$ . And  $\binom{n}{s} = \frac{n!}{(n-s)!s!}$ . So  $\binom{n}{s-1} + \binom{n}{s} = \frac{n!}{(n-s+1)!(s-1)!} + \frac{n!}{(n-s)!s!} = \frac{n!}{(n-s)!(s-1)!} (\frac{1}{n-s+1} + \frac{1}{s}) = \frac{n!}{(n-s)!(s-1)!} (\frac{s+n-s+1}{(n-s+1)s}) = \frac{n!(n+1)}{(n-s)!(s-1)!(n+1-s)s} = \frac{(n+1)!}{((n+1-s)s)!}$ . So therefore,  $\sum_{s=0}^{n+1} \{ \binom{n}{s-1} + \binom{n}{s} \} a^{n+1-s}b^s = \sum_{s=0}^{n+1} \binom{n+1}{s} a^{n+1-s}b^s$ . Note: if n is **-ve or fractional**,  $\binom{n}{r} = \frac{n(n-1)\dots(n-r+1)}{r!}$ . This sort of “*still makes sense*” and the Binomial Theorem (B.T.) does **extend** with care to these cases.

Applications of the B.T.: (1) **Counting subsets**. If X is a subset with n elements, then there are  $\binom{n}{r}$  different r element subsets. The **total number** of subsets of X is given by  $\sum_{r=0}^n \binom{n}{r} =$  (by the B.T.)  $= (1+1)^n = 2^n$ . Note:  $\binom{n}{r} = \binom{n}{n-r}$  since any **r element subset** of X determines and is *determined* by its complement which has n-r elements. (2) The **alternating** sum of the binomial coefficients is zero:  $\sum_{r=0}^n (-1)^r \binom{n}{r} = 0$ ; it is  $(1+(-1))^n$ .

### Tutorial

**Q:** A **sequence** is defined by  $u_1 = 1$ ,  $u_2 = 2$ , and if  $n > 2$ , then  $u_n = u_{n-1} + u_{n-2}$ , so each term is the sum of the previous two terms in the sequence. Prove that  $u_n < (\frac{7}{4})^n$  for all n. **A:** We are **given**  $u_1 = 1 < \frac{7}{4}$  and  $u_2 = 2 < \frac{49}{16} = (\frac{7}{4})^2$ . So suppose that *we know that*  $u_{n-1} < (\frac{7}{4})^{n-1}$  and that  $u_{n-2} < (\frac{7}{4})^{n-2}$ . **Then**  $u_n = u_{n-1} + u_{n-2} < (\frac{7}{4})^{n-1} + (\frac{7}{4})^{n-2} = (\frac{7}{4})^{n-2}(\frac{7}{4} + 1) = (\frac{7}{4})^{n-2}(\frac{11}{4})$ . *But*,  $\frac{11}{4} = \frac{44}{16} < \frac{49}{16} = (\frac{7}{4})^2$ . So  $u_n < (\frac{7}{4})^{n-2}(\frac{7}{4})^2 = (\frac{7}{4})^n$ . The result follows by *induction*.

**Remarks:** the expression  $u_n = u_{n-1} + u_{n-2}$  gives us a “*lever*” to find out about all  $u_n$  provided we know about the *first* two. If you like, you can think of the general inductive step as instructions on how to write out a **lengthy** proof on any particular case. For instance, if we *needed*  $u^{10} < (\frac{7}{4})^{10}$ , then we **have**  $u_1 = 1 < \frac{7}{4}$ ,  $u_2 < (\frac{7}{4})^2$  so  $u_3 < \frac{7}{4} + (\frac{7}{4})^2 = \frac{7}{4}(\frac{7}{4} + 1) = \frac{7}{4} \cdot \frac{11}{4} < (\frac{7}{4})^3$ . **Now**  $u_4 = u_3 + u_2 < (\frac{7}{4})^3 + (\frac{7}{4})^2 = (\frac{7}{4})^2(\frac{7}{4} + 1) = (\frac{7}{4})^2 \cdot \frac{11}{4} < (\frac{7}{4})^4$ , .... and **so** on. As we now have a *recipe* for how to write out such a proof, we are now **sure** that there is a (lengthy) proof that  $u_n < (\frac{7}{4})^n$ , so it **must** be true for any  $n$  ( $n =$  natural number).

**Q:** Let  $p_1 = 2, p_2 = 3, \dots$  be the **list** of primes arranged in increasing order. Consider the products of the *form*  $(p_1 \times \dots \times p_n) + 1$ . Show that this number is **prime** for  $n = 1$  to 5 but is not prime for  $n = 6$ . What prime *factors* does it have? **A:** The numbers are 3, 7, 31, 211, 2311 — **all** of which are prime. The *next* is  $30031 = 59 \times 509$ , so is not prime.

**Show** that if  $\gcd(a,c) = 1 = \gcd(b,c)$ , then  $\gcd(ab,c) = 1$ . **A:** If  $\gcd(a,c) = 1$ , there are numbers  $r,s$  *such that*  $ar+cs = 1$  (1). If  $\gcd(b,c) = 1$ , there are  $r',s'$  *such that*  $br'+cs' = 1$  (2). **Multiplying** through (1) by  $b$ , we have  $abr+cbcs = b$  (1'). *Multiply* this by  $r'$  giving  $ab(rr')+c(bsr') = br'$  (1''). Add  $cs'$  and use (2):  $ab(rr')+c(bsr'+s') = 1$ . So  $\gcd(ab,c) = 1$ . Note: We have often used that  $\gcd(a,c) = 1$  **implies** that there are  $r,s$  with  $ar+cs = 1$ . Here & elsewhere, we're also using *something* in the converse direction: if we're given  $a,c$  & can find  $r,s$  s.t.  $ar+cs = 1$ , then  $\gcd(a,c) = 1$ . **Why?** Here is a *proof*: **suppose that**  $t|a$  and  $t|c$ , then  $t|(ar+cs)$  so  $t|1$  and  $t = \pm 1$ . As  $d = \gcd(a,c)$  *divides* both  $a$  and  $c$ , and  $d > 0$ , then  $d = 1$ . Don't forget this simple argument — it makes life very **easy** sometimes!

19th February 1999

## Arithmetic Progression

$a, a+d, a+2d, \dots, a+(n-1)d$ . **Note:** here,  $a_k = a_{k-1} + d$ , where the **common** difference is  $d$ .  $a_1 = 1$  so (proof by *induction*)  $a_n = 1 + (n-1)d$ . **Formula:**  $S_n = \sum_{k=1}^n a_k = \frac{n}{2}(2a + (n-1)d)$ . Simple **proof** for this: we know  $S_n = a + (a+d) + \dots + (a+(k-1)d) + \dots + a + (n-1)d$ . And **also** (writing in reverse order)  $S_n = (a+(n-1)d) + (a+(n-2)d) + \dots + a$ . So **adding** these under each other,  $2S_n = (2a + (n-1)d) + (2a + (n-1)d) + \dots + \dots + (2a + (n-1)d)$ . So  $2S_n = n(2a + (n-1)d)$ . Hence we **have** the formula.

**Proof of formula by induction:**  $S_1 = a_1 = a$ . **Formula** gives  $\frac{1}{2}(2a + (1-1)d) = a$ . They agree! Assume  $S_n = \frac{n}{2}(2a + (n-1)d)$  for some  $n$ . And we *note* that  $S_{n+1} = S_n + a_{n+1} = S_n + a + ((n+1)-1)d = S_n + a + nd =$  (using the *inductive* hypothesis)  $= \frac{n}{2}(2a + (n-1)d) + a + nd = na + \frac{n(n-1)d}{2} + a + nd = (n+1)a + \frac{(n^2 - n + 2n)d}{2} = (n+1)a + \frac{(n^2 + n)d}{2} = \frac{(n+1)}{2}(2a + ((n+1)-1)d)$ . So the result **follows** by induction.

22nd February 1999

**Applications.** (1) The sum of the *first*  $n$  natural numbers is  $\frac{n(n+1)}{2}$ . [ $1+2+3+\dots+n = \frac{n(n+1)}{2}$ ]. [ $d = 1, a = 1$ ]. (2) The sum of the **first**  $n$  odd numbers is  $1+3+5+\dots+(2n-1)$ . Here  $a = 1$  and  $d = 2$  so  $S_n = \frac{n}{2}(2 + (n-1)2) = n^2$ . **Even:**  $2+4+6+\dots+2n = 2(\frac{n}{2})(n+1) = n^2 + n$ . So  $1+2+3+\dots+2n = \frac{2n(2n+1)}{2} = 2n^2 + n$  as *expected*.

## Geometric Progression

$S_n = a + ar + ar^2 + \dots + ar^{n-1}$  ( $r \neq 1$ ).  $S_n = \frac{a(1-r^n)}{1-r}$ . *Derivation:*  $a + ar + \dots + ar^{n-1} = S_n$ .  $ar + ar^2 + \dots + ar^n = rS_n$ .  $(1-r)S_n = a - ar^n$ ;  $S_n = [a(1-r^n)]/[1-r]$ . Proof by *induction* later.

**Sum of squares.**  $\sum_{k=1}^n k^2 = ?$  Claim:  $1^2+2^2+3^2+\dots+n^2 = \frac{n(n+1)(2n+1)}{6}$ . This is *clearly* true for  $n = 1$ . Assume true for some  $n$ , and look at  $1^2+\dots+n^2+(n+1)^2 = [1^2+2^2+\dots+n^2]+(n+1)^2$ . Using our **inductive** assumption,  $[1^2+2^2+\dots+n^2] + (n+1)^2 = \frac{n(n+1)(2n+1)}{6} + (n+1)^2$ . We *need*  $\frac{(n+1)(n+2)(2n+3)}{6}$ . Now  $\frac{n(n+1)(2n+1)}{6} + (n+1)^2 = \frac{(n+1)(n(2n+1)+6(n+1))}{6} = \frac{(n+1)(2n^2+n+6n+6)}{6} = \frac{(n+1)}{6}(2n^2+7n+6) = \frac{(n+1)}{6}(n+2)(2n+3)$  as required. The **validity**  $\forall n$  follows by *induction*.

**Sums of cubes.**  $\sum_{k=1}^n k^3 = \frac{n^2(n+1)^2}{4} = (\sum_{k=1}^n k)^2$ . Look at  $1^3+2^3 = 1+8 = 9$  ( $1+2 = 3$ ). And  $1^3+2^3+3^3 = 36$  ( $1+2+3 = 6$ ). And  $1^3+2^3+3^3+4^3 = 100$  ( $1+2+3+4 = 10$ ). Looking at the *table*, this suggests a quartic in  $n$  i.e.  $a_0n^4 + a_1n^3 + a_2n^2 + a_3n + a_4 = S_n$ . We **know** that  $a_0+a_1+a_2+a_3+a_4 = 1$  (Sub.  $n = 1$ ) and  $16a_0+8a_1+4a_2+2a_3+a_4$ , etc., giving *5 equations in 5 unknowns*. Solve e.g. by Gaussian elimination to get a (guessed) **solution** for  $S_n$ , then proof by *induction*.

n	S <sub>n</sub>					
1	1					
		8				
2	9		19			
		27		18		
3	36		37		6	
		64		24		0
4	100		61		6	
		125		30		
5	225		91			
		216				
6	441					

24th February 1999

## Tutorial

**Q:** Prove by **induction** that  $n! > 2^n$  for all  $n > 3$ . **A:** We start by checking the *statement* for  $n = 4$ .  $4! = 4 \times 3 \times 2 \times 1 = 24 > 16 = 2^4$ . So this is **correct**. Assume now that  $n! > 2^n$  for some  $n$ . Then  $(n+1)! = (n+1)n! > (n+1)2^n$ . But as  $n \geq 4$ ,  $n+1 > 2$ . So this is  $> 2 \cdot 2^n = 2^{n+1}$ . The validity of the formula **follows** by induction.

**Q:** A *sequence* is defined by  $u_1 = 4$ ,  $u_{n+1} = (u_n+6)^{1/2}$ . **Prove** (i)  $u_n > 3$  for all  $n$ , (ii)  $u_{n+1} < u_n$  for **all**  $n$ . **A:** (i)  $u_1 = 4 > 3$  so it's true for  $n = 1$ . Assume  $u_n > 3$  for some  $n$ . Then,  $u_{n+1} = (u_n+6)^{1/2} > (3+6)^{1/2} = 9^{1/2} = 3$ . So we *know that*  $u_n > 3$  is true for all  $n \geq 1$  by **induction**. For (ii),  $u_2 = \sqrt{10} < \sqrt{16} = 4$  so this is **true** for  $n = 1$ . Assume true for some  $n$ , i.e.  $u_{n+1} < u_n$ . Then,  $u_{n+1}+6 < u_n+6$  and as  $u_n > 3 > 0$ , we know that  $\sqrt{u_{n+1}+6} < \sqrt{u_n+6}$  i.e.  $u_{n+2} < u_{n+1}$ . Thus the result follows by **induction**.

26th February 1999

## Section 3: Basic Algebraic Structures

(Note: **Assume** e.g. ' $\cdot$ ' for  $\mathbf{R}$ ).  $\mathbf{Q}$  = the field of *rational* numbers.  $\mathbf{R}$  = the field of *real* numbers.  $\mathbf{C}$  = the field of *complex* numbers. Common properties of these and the integers modulo a prime number ( $\mathbf{Z}_p$ ): see later. We write  $F$  to stand for any of them ( $F$ , a field). Two *binary* operations:  $+$ :  $F \times F \rightarrow F$  [ $(a,b) \rightarrow (a+b)$ ]. This is *addition*. And  $\cdot$  (dot):  $F \times F \rightarrow F$  [ $(a,b) \rightarrow ab$ ]. This is *multiplication*. The two operations **satisfy** the following laws:

**Additive** Laws. (A1)  $a+b = b+a \forall a,b \in F$  (COMMUTATIVE). (A2)  $(a+b)+c = a+(b+c) \forall a,b,c \in F$  (ASSOCIATIVE). (A3)  $\exists 0 \in F$  s.t.  $0+a = a$ . (Existence of *additive neutral element* i.e. zero). (A4) Given  $a \in F$ ,  $\exists b \in F$  such that  $a+b = 0$ . (Existence of an **additive** inverse).

**Multiplicative** Laws. (M1)  $ab = ba \forall a,b \in F$  (COMMUTATIVE law for  $\cdot$ ) (M2)  $(ab)c = a(bc) \forall a,b,c \in F$  (ASSOCIATIVE). (M3)  $\exists 1 \in F$  s.t.  $1a = a \forall a \in F$  (*Existence of a unit element* 1).

Interaction of **addition** and **multiplication** laws: for all  $a, b, c$ ,  $a(b+c) = ab+ac$  (*DISTRIBUTIVE* law). Field axiom: If  $a \in F$ ,  $a \neq 0$ , then  $\exists b$  s.t.  $ab = 1$ . (Existence of *multiplicative* inverse for non-zero elements). Note: Both in A4 and here, the inverse is **unique**.

If  $ab = 1$  then  $ba = 1$  (M1). Suppose that  $ab' = 1$  as well. Then  $b(ab') = b1 = (\text{By M3}) = b = (\text{M2}) = (ba)b' = 1b' = b'$ . So  $b' = (\text{M3}) = 1b' = (ba)b' = (\text{M2}) = b(ab') = b1 = (\text{M3}) = b$ . We usually write  $-a$  for the element such that  $a+(-a) = 0$ , and  $a^{-1}$  for the **element** such that  $a.a^{-1} = 1$ .

$(\mathbf{Z}, +, \cdot)$  satisfies A1-A4, M1-M3 and D (not F, the field axiom). This is a COMMUTATIVE RING. We'll see later that the **set** of polynomials with coefficients in  $\mathbf{Q}$ ,  $\mathbf{R}$ ,  $\mathbf{C}$ , or any field  $F$ , form a *commutative* ring, and many properties of integers go across to here.

## Properties of $\mathbf{Q}$ and $\mathbf{R}$

$\mathbf{Q}$  and  $\mathbf{R}$  are both fields.  $\mathbf{Q}$  is a "subfield" of  $\mathbf{R}$ . But, if  $p$  is prime,  $\sqrt{p}$  is **not** an element of  $\mathbf{Q}$  (But *IS* an element of  $\mathbf{R}$ ). So  $\mathbf{R}$  is *bigger* than  $\mathbf{Q}$  (Much, MUCH bigger).

1st March 1999

## Properties of $\mathbf{C}$

**Recalling**,  $\mathbf{C} = \{a+ib \mid a, b \in \mathbf{R}\}$ .  $i$  is a symbol *satisfying*  $i^2 = -1$ . Addition:  $(a+ib) + (c+id) = (a+c) + i(b+d)$ . *Multiplication*:  $(a+ib)(c+id) = ac + iad + ibc + i^2bd = (ac-bd) + i(ad+bc)$ . We **write**  $z = a+ib$ , where  $\text{Re } z = a$  (Real part of  $z$ ) and  $\text{Im } z = b$  (Imaginary part of  $z$ ).

Let us verify a **field** axiom for  $\mathbf{C}$ : Associativity of  $+$ :  $((a_1+ib_1)+(a_2+ib_2))(a_3+ib_3) = (a_1+a_2) + i(b_1+b_2) + a_3+ib_3 = ((a_1+a_2)+a_3) + i((b_1+b_2)+b_3) = (a_1+(a_2+a_3)) + i(b_1+(b_2+b_3))$  by *corresponding* result in  $\mathbf{R} = \dots$ , etc. Associativity of multiplication is more complex.  $((a_1+ib_1).(a_2+ib_2)).(a_3+ib_3) = ((a_1a_2-b_1b_2)+i(b_1a_2+a_1b_2)).(a_3+ib_3) = \dots$  Now *expand*  $(a_1+ib_1)((a_2+ib_2).(a_3+ib_3))$  and **compare** the results.

*Division* (by non-zero elements). Solve  $(a+ib)(x+iy) = 1$ , (Note:  $1 = 1+i0$ ), where  $a+ib$  is non zero, which **means** that  $a$  and  $b$  are not both zero. So  $ax-by + i(ay+bx) = 1$  i.e.  $ax-by = 1$  (i) and  $ay+bx = 0$  (ii). (ii) **gives**  $ay = -bx$ . But now we must have *two* similar cases:  $a \neq 0$  and  $b \neq 0$ . For  $a \neq 0$ ,  $y = -bx/a$ , then (i) implies that  $ax - b^2/a = 1$ , or  $x^{(a^2-b^2)/a} = 1$ , or  $x = a/a^2-b^2$ . Then  $y = -b/a^2-b^2$ . So  $(a+ib)^{-1} = a-ib/a^2+b^2$ . (The other case gives the **same** answer).

Now write  $\bar{z} = a-ib$  (The **complex conjugate** of  $z$ ).  $z\bar{z} = a^2+b^2$ , which is *real*. And also  $|z| = \sqrt{(z\bar{z})}$  (The *modulus* of  $z$ ). If  $|z|$  is non zero, **then**  $z$  is non zero, and therefore  $z^{-1} = 1/z = \frac{\bar{z}}{z\bar{z}} = \frac{\bar{z}}{|z|^2}$ .

Solving *linear* equations over  $\mathbf{C}$ .  $\mathbf{Q}$ : Solve  $(2+i)x = 1-2i$  for  $x$ . **PLAN**: Find the **inverse** of  $2+i$ .  $|z|^2 = 2^2+1^2 = 5$ . So  $(2+i)^{-1} = 2/5-i/5$ . So  $x = (1-2i)(2/5-i/5)$ ,  $x = (2/5-2/5)+i(-4/5-1/5) = -i$ . **Check**:  $-i(2+i) = 1-2i$ . *Correct*.

## Workshop: Complex Numbers

**Express** in the form  $x+iy$  (i)  $(1+2i)(3+4i)$  and (ii)  $(2+i)^4$ . A: (i)  $(1+2i)(3+4i) = 3+4i+6i+8i = 3+10i-8 = -5+10i$ . (ii)  $(2+i)^4 = (2+i)^2(2+i)^2 = (4+4i+i^2)(4+4i+i^2) = (3+4i)(3+4i) = 9+12i+12i+16i^2 = 9+24i-16 = -7+24i$ .

**Q: Work** out  $(1+i)^n$  for  $n = 20$  and  $n = 22$ . Find four *complex* numbers  $z$  satisfying  $x^4 = -1$ . A: We use the *fact* that  $(1+i)^{22} = ((1+i)^{11})^2$ . But we can get  $(1+i)^{11}$  from  $(1+i)(1+i)^{10}$  which we evaluate on the *route* to getting  $(1+i)^{20} = ((1+i)^{10})^2 = (((1+i)^5)^2)^2$ . We get  $(1+i)^5$  by hand, then square it *twice* to get  $(1+i)^{20} = -1024$ . Using the above method,  $(1+i)^{22} = -2048i$ . To get the 4 complex numbers, we *notice* that  $(1+i)^4 = -4$ , so  $\frac{1}{4}(1+i)^4 = -1$ . Taking the  $\frac{1}{4}$  inside,  $(1+i/\sqrt{2})^4 = -1$ , so  $x = 1+i/\sqrt{2}$ . We get the other **roots** by multiplying by  $-1$ ,  $i$  and  $-i$  to get the *solution* set  $\{1+i/\sqrt{2}, -1-i/\sqrt{2}, 1+i/\sqrt{2}, 1-i/\sqrt{2}\}$ .

**Q: Which of the following** sets is the solution set of the equation  $z^4 = 1$  ( $z$  is a complex number)?: A =  $\{1\}$ , B =  $\{1+i/\sqrt{2}, -1-i/\sqrt{2}, 1+i/\sqrt{2}, 1-i/\sqrt{2}\}$ , C =  $\{1, -1\}$ , D =  $\{1, i\}$ , E =  $\{1, -1, i, -i\}$ , F =  $\{1+i/\sqrt{2}, 1-i/\sqrt{2}\}$ . A: It is E — we need **4** solutions (4 roots) and we *need the roots 1 and -1* — only solution E has all these requirements.

## Assignment 2

**Q: The fibonacci** series is defined by  $u_1 = u_2 = 1$ ,  $u_{n+1} = u_n + u_{n-1}$ . Show that for any  $n$ ,  $u_n$  and  $u_{n+1}$  are coprime. A: as  $u_1$  &  $u_2$  are both 1, their g.c.d. is 1, so the **statement** is true for  $n = 1$ . Assuming it is true for  $n$  i.e. that  $\gcd(u_n, u_{n+1}) = 1$ , *examine*  $\gcd(u_{n+1}, u_{n+2}) = d$ , say. If  $d|u_{n+1}$  and  $d|u_n$ , then  $d|\gcd(u_n, u_{n+1})$  also. As  $d$  is **positive** and divides 1, it is 1 i.e.  $\gcd(u_{n+1}, u_{n+2}) = 1$  as required. The result follows by **induction**.

**Q: Given**  $x_0 = 2$ ,  $x_1 = 5$ , and  $x_{n+2} = 5x_{n+1} - 3x_n$  for  $n \geq 0$ , prove that  $2^n x_n = (5+\sqrt{13})^n + (5-\sqrt{13})^n$  for any *natural* number  $n$ . A: For  $n = 0$ , the **formula** gives  $2^0 x_0 = (5+\sqrt{13})^0 + (5-\sqrt{13})^0 = 1+1 = 2$ . So the formula **holds** for  $n = 0$ . For  $n = 1$ , the formula gives  $2x_1 = 2^1 x_1 = (5+\sqrt{13})^1 + (5-\sqrt{13})^1 = 5+5 = 10$ . So  $x_1 = 5$  and that is **correct**.

For this type of problem, the form of induction assumes that *two consecutive cases* of the formula are true, and derives the next. (It always requires two base cases as we have declared above). Assume that the formula is valid for  $x_n$  and  $x_{n+1}$  so we may assume that  $2^n x_n = (5+\sqrt{13})^n + (5-\sqrt{13})^n$  and  $2^{n+1} x_{n+1} = (5+\sqrt{13})^{n+1} + (5-\sqrt{13})^{n+1}$ .

Now we **examine**  $2^{n+2} x_{n+2} = 2^{n+2}(5x_{n+1} - 3x_n) = 10(2^{n+1} x_{n+1}) - 12(2^n x_n) = 10(5+\sqrt{13})^{n+1} + 10(5-\sqrt{13})^{n+1} - 12(5+\sqrt{13})^n - 12(5-\sqrt{13})^n = [10(5+\sqrt{13})(5+\sqrt{13})^n - 12(5+\sqrt{13})^n] + [10(5-\sqrt{13})(5-\sqrt{13})^n - 12(5-\sqrt{13})^n] = (50-12+10\sqrt{13})(5+\sqrt{13})^n + (50-12-10\sqrt{13})(5-\sqrt{13})^n = (38+10\sqrt{13})(5+\sqrt{13})^n + (38-10\sqrt{13})(5-\sqrt{13})^n$ . Now we need to *compare this* to what we want — need  $(5+\sqrt{13})^2$  more in front of  $(5+\sqrt{13})^n$ . We have  $38+10\sqrt{13}$ .

We note that  $(5+\sqrt{13})^2 = 25+10\sqrt{13}+13 = 38+10\sqrt{13}$ , whilst  $(5-\sqrt{13})^2 = 38-10\sqrt{13}$ , so the formula for the **cases**  $n$  &  $n+1$  give  $2^{n+2} = (5+\sqrt{13})^2(5+\sqrt{13})^n + (5-\sqrt{13})^2(5-\sqrt{13})^n = (5+\sqrt{13})^{n+2} + (5-\sqrt{13})^{n+2}$  as hoped for. The result **holds** for all  $n$  by induction.

**Q:** Prove by induction that the Geometric Progression formula holds. That is, given real  $a$  and  $r$ , with  $r \neq 1$ , prove that the **sum** of the finite geometric series starting at  $a$  with ratio  $r$  is given by  $\sum_{i=0}^{n-1} ar^i = (a(1-r^n))/(1-r)$  for all  $n \geq 1$ . **A:** For  $n = 1$ , the geometric series is simply  $ar^0 = a$ . The RHS of the formula **likewise** yields  $a = (a(1-r^1))/(1-r)$ , so this case of the *formula* is valid.

**Assume** that the formula is true for the sum to  $ar^{n-1}$  i.e.  $\sum_{i=0}^{n-1} ar^i = (a(1-r^n))/(1-r)$ . The sum to the **term**  $ar^n$  will be  $\sum_{i=0}^n ar^i = \sum_{i=0}^{n-1} ar^i + ar^n$ . By our **inductive** hypothesis, this equals  $(a(1-r^n))/(1-r) + ar^n = \frac{a((1-r^n)+(1-r)r^n)}{1-r} = \frac{a(1-r^n+r^n-r^{n+1})}{1-r} = \frac{a(1-r^{n+1})}{1-r}$  as hoped for, i.e. the **formula** for the sum of  $n$  terms implied the formula for the sum of  $n+1$  terms. The *validity* of the formula for all  $n$  therefore follows by induction.

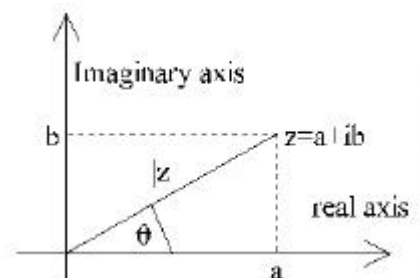
5th March 1999

## Solving Simple Systems of Linear Equations

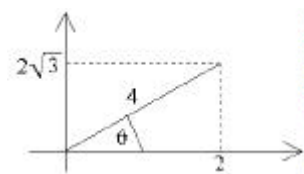
**Example:**  $(2+i)x + (1+2i)y = 3$  and  $ix + (3-i)y = 6+i$ . **Multiply** the first equation by  $(2+i)^{-1}$  i.e.  $(2/5 - i/5)$  to give  $x + (2/5 - i/5)(1+2i)y = 6/5 - 3i/5$ , or  $x + (4/5 + 3i/5)y = 6/5 - 3i/5$ . Now multiply the *second equation* by  $(-i)$  to give  $x + (-1-3i)y = 1-6i$ . Add the **two** results we get to give  $(4/5 + 1 + (3/5 + 3)i)y = 6/5 - 1 + (-3/5 + 6)i$ . **Simplify** and solve for  $y$ ; *substitute* this solution in the others and check.

## The Argand Diagram

Also called the *complex plane*. We represent  $a+ib$  by a point with **cartesian** co-ordinates,  $(a,b)$ .  $|z|$  becomes the distance of  $z$  from the origin. We **use**  $\theta$  to denote the angle between the line  $Oz$  and the +ve Real axis. Then  $a = |z|\cos\theta$ ,  $b = |z|\sin\theta$ ,  $z = |z|(\cos\theta + i\sin\theta)$  (**provided**  $z \neq 0$ ). The angle  $\theta$  is called the **argument** of  $z$ , and is written as ' $\arg(z)$ '. By convention,  $-\pi < \theta \leq \pi$ . Thus to specify a non-zero **complex** number, we can choose polar co-ordinates  $(r, \theta)$ , where  $r = |z|$ ,  $\theta = \arg(z)$ , and  $z = r(\cos\theta + i\sin\theta)$ .



**Example:**  $a = 2$ ,  $b = 2\sqrt{3}$ . So  $|z| = (4+12)^{1/2} = \sqrt{16} = 4$ .  $\cos\theta = 2/4 = 1/2$ , and  $\sin\theta = 2\sqrt{3}/4 = \sqrt{3}/2$ . So  $\theta = \pi/3 = \arg(z)$ . Note: for a **real** number  $a$ , then  $a$  is thought of as  $a+i0$ , and  $\arg(a)$  is either  $0$  (for  $a > 0$ ) or  $\pi$  (for  $a < 0$ ) It is **undefined** if  $a = 0$ .



*Multiplication of complex numbers in polar form.*  $r_1(\cos\theta_1 + i\sin\theta_1) \times r_2(\cos\theta_2 + i\sin\theta_2) = r_1 r_2 [(\cos\theta_1 \cos\theta_2 - \sin\theta_1 \sin\theta_2) + i(\cos\theta_1 \sin\theta_2 + \sin\theta_1 \cos\theta_2)] = r_1 r_2 (\cos(\theta_1 + \theta_2) + i\sin(\theta_1 + \theta_2))$ . **Multiply** the Moduli, Add the Arguments.

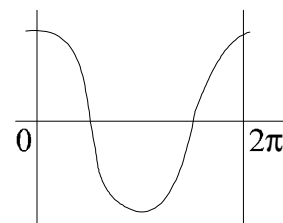
## De Moivre's Theorem

**If**  $z = r(\cos\theta + i\sin\theta)$ , then for *any*  $n \in \mathbf{Z}$ ,  $z^n = r^n(\cos n\theta + i\sin n\theta)$ .

**Proof.** Case  $n \geq 0$ : by *induction*. True for  $n = 1$  — this is clear. If true for  $n$  in general, then  $z^n = r^n(\cos n\theta + i \sin n\theta)$ . Now  $z^{n+1} = z^n \cdot z = r^n(\cos n\theta + i \sin n\theta) \cdot r(\cos \theta + i \sin \theta) = r^{n+1}(\cos(n\theta + \theta) + i \sin(n\theta + \theta))$  [MMAA], etc. For  $n < 0$ ,  $n = -m$ , &  $z^n = 1/z^m$ . So  $\frac{1}{r^m(\cos m\theta + i \sin m\theta)} = \frac{r^{-m}(\cos m\theta - i \sin m\theta)}{\cos^2 m\theta + i \sin^2 m\theta} = r^n(\cos n\theta + i \sin n\theta)$ .

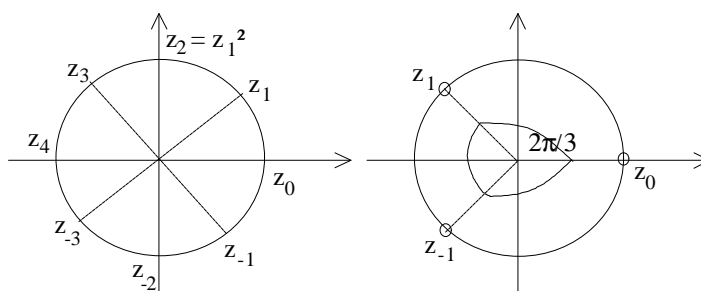
**Applications.** (1) We know  $\cos 2\theta = \dots$  and  $\sin 2\theta = \dots$  **What** about  $\cos 5\theta$  and  $\sin 5\theta$  in terms of  $\cos \theta$  and  $\sin \theta$ ? Using the theorem,  $\cos 5\theta + i \sin 5\theta = (\cos \theta + i \sin \theta)^5$ . Now we **know** that  $(a+b)^5 = a^5 + 5a^4b + 10a^3b^2 + 10a^2b^3 + 5ab^4 + b^5$ . So  $(\cos \theta + i \sin \theta)^5 = \cos^5 \theta - 10\cos^3 \theta \sin^2 \theta + 5\cos \theta \sin^4 \theta + i(5\cos^4 \theta \sin \theta - 10\cos^2 \theta \sin^3 \theta + \sin^5 \theta)$ .

(2) **Complex** roots of numbers. Solving the equation  $z^n = a$  ( $a$  is a **complex** number). For  $z^n = 1$ , put  $z = r(\cos \theta + i \sin \theta)$ . So  $z^n = 1 \Rightarrow r^n(\cos n\theta + i \sin n\theta) = 1$ . **Remember**, because  $r > 0$  and  $r \in \mathbf{R}$ , then  $r^n = 1 \Rightarrow r = 1$ . Comparing *real* with *real*, *imaginary* with *imaginary*,  $\cos n\theta = 1$  &  $\sin n\theta = 0$ .  $\cos n\theta = 1$  iff  $n\theta$  is a multiple of  $2\pi$ :  $n\theta = 2k\pi$ ,  $k = 0, \pm 1, \pm 2, \dots$   $\sin n\theta = 0$  at **all** these points. Thus  $n\theta = 2k\pi$ ;  $k = 0, \pm 1, \pm 2, \pm 3$  etc., so  $\theta = \frac{2k\pi}{n}$ .



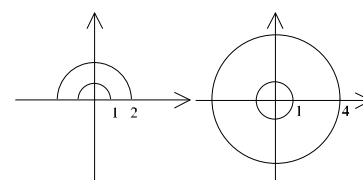
**Write**  $\theta_k = \frac{2k\pi}{n}$ . Now,  $-\pi < \theta \leq \pi$ . We have  $n$  *different* solutions to this. Two cases:  $n$  even ( $n = 2m$ , say).  $\theta_0 = 0$ ,  $\theta_1 = \frac{2\pi}{n}$ ;  $\theta_2 = \frac{4\pi}{n}$ , ...,  $\theta_m = \frac{2m\pi}{n} = \pi$ . If  $k > m$ , then  $\theta_k > \pi$ . And  $\theta_{-1} = -\frac{2\pi}{n}$ ,  $\theta_{-2} = -\frac{4\pi}{n}$ ,  $\theta_{-(m+1)} = -\frac{2(m+1)\pi}{n}$ .  $\theta_{-m} = -\pi$ , so **outside the range**. For the  **$z$ 's** themselves,  $z_k = \cos \theta_k + i \sin \theta_k$ . Note that using  $\theta_k$  without restriction, we get  $z_m = z_{-m}$ ,  $z_{m+1} = z_{-(m+1)}$ . The **illegal**  $\theta_k$  correspond to the solutions **already** in the list:  $z_{-(m+1)} \dots z_0 \dots z_m$ . Similarly for the **odds**, ( $n = 2m+1$ , say),  $\theta_0, \theta_1, \theta_2, \dots, \theta_m = \frac{2m\pi}{n}$ .  $\theta_{-1}, \dots, \theta_{-m} = -\frac{2m\pi}{n}$ .

**Example:**  $n = 8$  (so  $m = 4$ ).  $z_k = \cos \theta_k + i \sin \theta_k$ .  $z^8 = 1$ .  $\theta_0 = 0$  so  $z_0 = 1$ .  $\theta_1 = \frac{2\pi}{8}$  so  $z_1 = \frac{1}{\sqrt{2}} + i \frac{1}{\sqrt{2}}$ .  $\theta_2 = \frac{4\pi}{8}$  so  $z_2 = i$ ;  $\theta_3 = \frac{6\pi}{8}$ ,  $\theta_4 = \frac{8\pi}{8}$ . The pictures show the *cases*  $n = 8$  (left) **and**  $n = 3$  (right). Notes: For the picture on the *left*,  $z_1 = \frac{1}{\sqrt{2}} + i \frac{1}{\sqrt{2}}$ ,  $z_3 = -\frac{1}{\sqrt{2}} + i \frac{1}{\sqrt{2}}$ ,  $z_{-3} = -\frac{1}{\sqrt{2}} - i \frac{1}{\sqrt{2}}$ , and  $z_{-1} = \frac{1}{\sqrt{2}} - i \frac{1}{\sqrt{2}}$ .



### Workshop

**Q:** Draw the **following** region of the complex plane (given in polar co-ordinates):  $\{(r, \theta): 1 \leq r \leq 2, 0 \leq \theta \leq \pi\}$ . Draw the **image** of this set under the squaring function:  $x$  onto  $z^2$ , where  $z$  is a complex number  
**A:** See the pictures on the **right**.



**Q:** Some *useful* trigonometric identities are related via a combination of de Moivre's theorem and the **Binomial** theorem. Expand  $(\cos(\theta) + i \sin(\theta))^2$  in these **two** different ways. **A:** Expand using the **Binomial** theorem giving  $(\cos(\theta) + i \sin(\theta))^2 = \cos^2(\theta) - \sin^2(\theta) + i 2 \cos(\theta) \sin(\theta)$  and using de *Moivre*  $(\cos(\theta) + i \sin(\theta))^2 = (\cos(2\theta) + i \sin(2\theta))$ . Now compare real & imaginary parts to prove that the **two** formulae are the same. Similarly for  $(\cos(\theta) + i \sin(\theta))^n$ , where  $n = 3, 4, \dots$

**Roots** of complex numbers. If you have an *equation*  $z^n = a$ , where  $a$  is complex, the solution is obtained by writing  $a$  in **polar** form and trying  $z = r(\cos(\theta)+isin(\theta))$ . de Moivre's theorem then enables you to work out  $z^n$  in terms of  $r$  and  $\theta$  and on **comparing** this with the polar form of  $a$ , you get  $n$  *different* values of  $\theta$  that will give you the arguments of the  $n$  solutions of your original equation. The modulus will be the **usual** real  $n^{\text{th}}$  root of the modulus  $|a|$  of  $a$ . The various **values** of the arguments will be equally spaced *about* the circle of radius  $|a|^{1/n}$  and centre the origin.

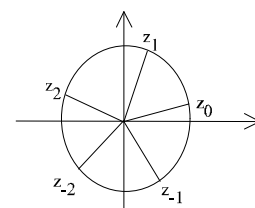
**Q: Solve** the equation  $z^6-2z^3+2 = 0$  ( $z$  complex). Hint: This is a *quadratic* equation in  $z^3$ , so solve  $w^2-2w+2 = 0$  for  $w$  and then solve  $z^3 = w$  for the two values of  $w$  you have **obtained**. **A:** Put  $w = z^3$  as *suggested*, then  $w = (*) 1 \pm i\sqrt{2}(\cos(\pi/4) \pm isin(\pi/4))$ . Let  $w_1 = 1+i$ ,  $w_2 = 1-i$  (This is  $\bar{w}$  of course) and first **solve**  $z^3 = w_1$ . (\*)  $w = \frac{2 \pm \sqrt{4-8}}{2} = \frac{2 \pm \sqrt{-4}}{2} = \frac{2 \pm 2i}{2} = 1 \pm i$ . **Thus**  $z = \sqrt[6]{2}(\cos(\theta)+isin(\theta))$  where  $3\theta = \pi/4 + 2k\pi$  and  $-\pi \leq \theta \leq \pi$ . Hence  $\theta = \pi/12, 3\pi/4$  (or  $9\pi/12, -7\pi/12$ ), giving **three** solutions. The other three are obtained by *repeating* the process with  $w_2$ . This gives the complex *conjugates* of the three solutions found **above**).

12th March 1999

Let  $z^n = c$ , where  $c$  is **any** complex number. Express  $c$  in *polar* form,  $c = \rho(\cos\phi+isin\phi)$ . Put  $z = r(\cos\theta+isin\theta) = \rho(\cos\phi+isin\phi)$ . Comparing the *moduli*,  $r^n = \rho$ . Now as  $r, \rho > 0$ , and are **real**, then  $r = \rho^{1/n}$ , the  $n^{\text{th}}$  root of  $r$ . Now look at  $\cos n\theta = \cos\phi$ ,  $\sin n\theta = \sin\phi$ . Consider the *graphs* of  $\sin$  and  $\cos$ . They imply  $n\theta$  and  $\phi$  differ by a multiple of  $2\pi$ . This implies that there is an *integer*  $k$  s.t.  $n\theta = 2k\pi + \phi$ ;  $\theta_k = \frac{2k\pi + \phi}{n}$ .

We get  $n$  **different**  $z_k = r(\cos\theta_k+isin\theta_k)$  corresponding to the  $n$  *values* of  $\theta_k$  in the range  $-\pi < \theta_k \leq \pi$ . **Example:** Solve  $z^5 = 1/\sqrt{2} + i/\sqrt{2}$ . Here,  $c = 1/\sqrt{2} + i/\sqrt{2}$ ,  $\rho = 1$  and  $\phi = \pi/4$ . So  $r = (1)^{1/5} = 1$ .  $n\theta_k = 2k\pi + \pi/4$ ;  $5\theta_k = 2k\pi + \pi/4$ ;  $\theta_k = \frac{2k\pi + \pi/4}{5}$ . Or perhaps more *conveniently*,  $5\theta_k = \frac{(8k+1)\pi}{4}$ ;  $\theta_k = \frac{(8k+1)\pi}{20}$ .

Now consider **the cases** of  $k$ .  $k = 0$ :  $\theta_k = \pi/20$ .  $k = 1$ :  $\theta_k = 9\pi/20$ .  $k = 2$ :  $\theta_k = 17\pi/20$ .  $k = 3$ :  $\theta_k = 25\pi/20$ , which is **more** than  $\pi$  and hence too big. Now  $k = -1$  gives  $\theta_k = -7\pi/20$ ;  $k = -2$  gives  $-15\pi/20$ . We have now obtained 5 solutions as expected. **Confirmation:**  $k = -3$  gives  $\theta_k = -23\pi/20$ ,  $< \pi$ ; hence too *small*. **Hence**  $z_n = \cos((8k+1)\pi/20) + isin((8k+1)\pi/20)$ . Look back at the  $n^{\text{th}}$  roots of 1:  $z_k = \cos(\frac{2k\pi}{n}) + isin(\frac{2k\pi}{n})$ .  $z_2 = z_1^2$ ,  $z_3 = z_1^3$ , ...,  $z_k = z_1^k$ . Now  $1 + z_k + z_k^2 + \dots + z_k^{n-1} = 0$ . **Why?**



## Polynomials over $\mathbf{R}$ ; over $\mathbf{C}$

$F$  will be a *field* (usually  $\mathbf{R}$  or  $\mathbf{C}$ ). Definition: A polynomial over  $F$  is an *expression* of the form  $\sum_{i=0}^n a_i x^i$  for some  $n$ , **where** the  $a_i$  are all elements of  $F$ . The set of *polynomials* over  $f$  are denoted by  $f(x)$ .

*Addition* of polynomials. If  $p(x) = \sum_{i=0}^m a_i x^i$  and  $q(x) = \sum_{j=0}^n b_j x^j$ , then  $p(x)+q(x) = \sum_{k=0}^N (a_k+b_k)x^k$ , where  $N = \max(m,n)$ . In the *range* between  $m$  and  $N$  (respectively  $n$  and  $N$ ),  $a_k = 0$  (and  $b_k = 0$ ). Example:  $p(x) = x+2$ ,  $q(x) = x^2+3x+0$ . (the  $+0$  is usually **omitted**).  $p(x)+q(x) = x^2+4x+2$  ( $m = 2$ ,  $n = 2$  so  $N = 2$ ). We have a *dummy* term  $0x^2$  in  $p(x)$ , so we have the same number of terms in  $p$  &  $q$ .

15th March 1999

**Multiplying Polynomials.** We know how to do this in *practice*: if  $p(x) = x+2$  and  $q(x) = x^2+3x+2$ , then  $p(x)q(x) = (x+2)(x^2+3x+2) = x^3+3x^2+2x+2x^2+6x+4 = x^3 + (3+2)x^2 + (2+6)x + 4 = x^3+5x^2+8x+4$ . **Abstractly**, or in general, if  $p(x) = \sum a_i x^i$  and  $q(x) = \sum a_j x^j$ , then  $p(x)q(x) = \sum c_k x^k$ , where  $c_k = \sum_{i+j=k} a_i b_j$ . With these **definitions** of  $+$ ,  $\cdot$ ,  $f[x]$  becomes a ring (i.e. Additive laws, Multiplicative laws, *Distributive* law (i.e.  $p(x)(q(x)+r(x)) = p(x)q(x)+p(x)r(x)$ ) but not the **Field** axiom).

## Degree

If  $p(x) = \sum_{i=0}^n a_i x^i$ , then  $\deg(p) = \max\{k \mid a_k \text{ not zero}\}$ . **Constants** are degree zero polynomials — except 0, which we take the *degree* of to be  $-\infty$ . **Properties** of degree: (i)  $\deg(p(x)q(x)) = \deg(p(x))+\deg(q(x))$ . (ii)  $\deg(p(x)+q(x)) \leq \max(\deg(p(x)), \deg(q(x)))$ .

*Division algorithm for polynomials. Theorem:* Given polynomials  $a(x), b(x) \in F[x]$ , then there are **polynomials**  $q(x), r(x)$  such that  $a(x) = b(x)q(x)+r(x)$  with  $\deg(r(x)) < \deg(b(x))$ . **Example:** Let  $a(x) = x^3+3x^2-x+4$  and  $b(x) = x+2$ . Here,  $\deg(a) = 3$  and  $\deg(b) = 1$ . Divide in the normal way, giving  $x^3+3x^2-x+4 = (x+2)(x^2+x-3)+10$ .

17th March 1999

## Tutorial

**Q:** Draw the **following** sets of *complex* numbers: (i)  $\{z \mid |z-3| = 3\}$ , (ii)  $\{z \mid |z-3| = |z-5|\}$ , (iii)  $\{z \mid |2z-i| = |z+2i|\}$ . **A:** (i) Now  $|z-a|$  is the *distance* from  $z$  to  $a$ .  $|z-a|^2 = (x-a_1)^2+(y-a_2)^2$  if  $a = a_1+ia_2$  and  $z = x+iy$ . In (i),  $a = 3 = 3+0i$ . So  $|z-3|^2 = (x-3)^2+y^2$ . Now in  $|z-3| = 3$ ,  $|z-3|^2 = 9$ ; so  $(x-3)^2+y^2 = 9$ . This is a circle **centred** at  $(3,0)$  with *radius* 3.

(ii) This is the set of  $z$  whose distance from 3 is the same as the *distance* from 5:  $|z-3| = |z-5|$ .  $|z-3|^2 = |z-5|^2$ .  $(x-3)^2+y^2 = (x-5)^2+y^2$ .  $(x-3)^2 = (x-5)^2$ .  $x^2-6x+9 = x^2-10x+25$ .  $4x = 16$ ;  $x = 4$ . (iii) Now  $|2z-i|^2 = 4x^2+(2y-1)^2$ ; and  $|z+2i|^2 = x^2+(y+2)^2$ . So *equating*,  $3x^2+3y^2-8y-3 = 0$ .  $x^2+y^2-\frac{8}{3}y-1 = 0$ .  $x^2+(y-\frac{4}{3})^2-\frac{16}{9}-1 = 0$ .  $x^2+(y-\frac{4}{3})^2 = \frac{25}{9}$ . This is another **circle** with *radius*  $\frac{5}{3}$ .

19th March 1999

## Assignment 3

When you have a **quadratic** equation you cannot factorise, and  $b^2-4ac < 0$ , use complex numbers to solve the equation. When solving sets of *linear* equations e.g.  $(3+4i)x+(2-2i)y = 0$ ,  $(2+2i)x+(3-4i)y = 0$ , multiply through or divide through to get one of the equations devoid of  $i$ 's in one variable. Then *manipulate* (see previous example).

**Q:** Solve  $u_n+2u_{n-1}+7u_{n-2} = 0$  with  $u_0 = -1, u_1 = 1$ . **A:** Try as usual  $u_n = A\lambda^n$  to get the corresponding *quadratic* equation in  $\lambda$ :  $\lambda^2+2\lambda+7 = 0$ . Solving gives  $\lambda = -1\pm i\sqrt{6}$ . So the **general** solution is  $u_n = A(-1+i\sqrt{6})^n+B(-1-i\sqrt{6})^n$ . Substitute in *initial* values from which we have two equations to solve for  $A$  &  $B$ , to give  $u_n = -\frac{1}{2}[(-1+i\sqrt{6})^n+(-1-i\sqrt{6})^n]$ . **Q:** Solve  $u_n+2u_{n-1}+3u_{n-2} = 0$  with  $u_0 = 0, u_1 = i$ . **A:** **Same** as above.

Let  $p(x) = x-2$ ,  $q(x) = x^3+3x^2-2x+16$ . Applying *long division* gives  $x^3+3x^2-2x+16 = (x-2)(x^2+5x+8)+32$ . This is of the **form**  $q(x) = p(x)a(x)+r(x)$ , with  $\deg(r(x)) < \deg(p(x))$ . Given  $p(x) \in F[x]$  and some element  $x \in F$ , we can then *substitute*  $\alpha$  in place of  $x$  in  $p(x)$ :  $p(x) = \sum_{i=0}^{\deg(p(x))} a_i x^i$ . For example, when  $q(x) = x^3+3x^2-2x+16$ , and  $\alpha = 2$ ,  $q(2) = 32$ . If  $p(\alpha) = 0$ , we say that  $\alpha$  is a root of the *polynomial*  $p$ .

**Theorem: the remainder theorem:** If  $p(x) \in F[x]$  and  $\alpha \in F$ , then the remainder on dividing  $p(x)$  by  $(x-\alpha)$  is exactly  $p(\alpha)$ . Proof: by the *division algorithm*,  $p(x) = (x-\alpha)q(x)+r(x)$  (\*), where  $\deg(r(x)) < \deg(x-\alpha)$ . So  $r(x)$  must be constant. Evaluate both **sides** at  $\alpha$ :  $p(\alpha) = (\alpha-\alpha)q(\alpha)+r(\alpha)$ . But as  $r(x)$  is constant ( $\deg \leq 0$ ),  $r(x)$  is equivalent to  $r(\alpha)$ . **Corollary:** If  $\alpha$  is a root of  $p(x)$ , then  $(x-\alpha)$  divides  $p(x)$ .

Note:  $x^2+2x+7 = 0$  cannot be **factorised** over **R**.  $p(x) = x^2+2x+7$  has *complex* roots  $-1+i\sqrt{6}$ ,  $-1-i\sqrt{6}$ . Working over **C**,  $p(x) = (x-\alpha_1)(x-\alpha_2)$ . But  $\alpha_1, \alpha_2$  are not in **R**, so  $p(x)$  cannot be factorised in **R[x]**. But it *can* be factorised in **C[x]**. Another case:  $p_2(x) = x^2-2$ . This is *Rational*. But it cannot be factorised in **Q[x]**. However, it can be factorised when considered as a *polynomial* over **R** or **C**, because  $p_2(x) = (x-\sqrt{2})(x+\sqrt{2})$ . We saw earlier that  $\sqrt{2}$  is **not** rational.

## Euclid's Algorithm for Polynomials

Given 2 **polynomials**  $f(x), g(x) \in F[x]$ , they have a g.c.d.  $d(x)$  which can be *written* in the form  $d(x) = \lambda(x)f(x)+\mu(x)g(x)$ . Proof: Look at the case for *integers* and rewrite the proof with polynomials instead of integers. Note: interpret degree as a measure of size. We can now find  $\gcd((f(x), g(x)))$  as in the case of **numbers**. (*Maple*: gcdex).

22nd March 1999

## Irreducible Polynomials

A **polynomial**  $p(x) \in F[x]$  is said to be *irreducible* over  $F$  if whenever  $p(x) = a(x)b(x)$ , with  $a(x), b(x) \in F[x]$ , then one of  $a(x)$  or  $b(x)$  has degree 0 (i.e. is a *constant*). Example:  $x^2-2$  is irreducible over **Q** because  $x^2-2$  can only be *written* as a product of polynomials, one of which is constant e.g.  $2(x^{2/2}-1)$ ; there are lots *more*: but  $\deg(2) = 0$ .

$x^2-2$  is not of the form  $(x-\alpha)(x+\beta)$  where  $\alpha, \beta \in \mathbf{Q}$ .  $(x^2+(\alpha+\beta)x+\alpha\beta) = x^2-2$ , so  $\alpha = -\beta$  and  $\alpha^2 = 2$ . But **no** such  $\alpha$  exists. With this, we get a unique factorisation theorem for polynomials. (For a statement of proof, you look at the **integer** case and do some fairly obvious changes). So irreducible polynomials are the *building blocks* for all polynomials in  $F[x]$ , thus it is important to see **what** polynomials are irreducible over the *main fields of interest* (i.e. **Q, R, C**).

Irreducible over Q (hard). We know that all  $x^2 \pm p$  are irreducible, as are all  $(x-a)$ . All  $ax^2+bx+c$  are **irreducible** if  $\sqrt{(b^2-4ac)}$  is not rational. For us — darkness. Irreducible over R: 2 forms:  $x^2+bx+c$  with  $b^2 < 4c$ , and  $(x-a)$ , with  $a \in \mathbf{R}$ . Over C: Just the linear *polynomials*  $(x-a)$ ,  $a \in \mathbf{C}$ . **Fundamental theorem of algebra:** A polynomial in  $\mathbf{C}[x]$  has all of its roots in **C** (Proof uses *complex* variable theory i.e. calculus over **C**).

**Remember:** If  $x^2+bx+c = (x-\alpha)(x-\beta)$ , then  $c = \alpha\beta$ ;  $b = -(\alpha+\beta)$ . And if  $x^3+bx^2+cx+d = (x-\alpha)(x-\beta)(x-\gamma)$ , then  $-d = \alpha\beta\gamma$ ;  $c = \alpha\beta+\beta\gamma+\alpha\gamma$ ;  $-b = \alpha+\beta+\gamma$ . These are the *symmetric functions* of order 3 in  $\alpha,\beta,\gamma$ , and this **generalises** for higher degree polynomials.

24th March 1999

**Q:** Find a **transformation**  $f(z) = \frac{az+b}{cz+d}$  such that  $f(3i) = 2+i$ ,  $f(1) = 1-i$ ,  $f(1+i) = 4$ . **A:** *Substitute in: (First condition):*  $2+i = \frac{a(3i)+b}{c(3i)+d}$ ;  $3ia+b = (2+i)(3ic+d)$ ;  $3ia+b = 6ic+2d-3c+id$ ;  $3ia+b = (6i-3)c + (2+i)d$ ;  $3ia + b + (3-6i)c + (-2-i)d = 0$ . Do the same for *condition 2:*  $1-i = \frac{a+b}{c+d}$ ;  $(c+d)(1-i) = a+b$ ;  $c(1-i)+d(1-i) = a+b$ . Now for the 3rd condition:  $4 = \frac{a(1+i)+b}{c(1+i)+d}$ ;  $a(1+i)+b = c(4+4i)+4d$ . Now we have 3 equations in 4 unknowns. Solve by *Gaussian elimination* and get the answer in terms of a **parameter**.

26th March 1999

## Modular Arithmetic: Introduction

**Q:** No **integer** of the form  $4k+3$  can be written as a sum of two squares — why not? To answer this, let us first look at the *even* and *odd* numbers. Let us call even numbers as having zero remainder after division by 2,  $[0]_2$ . Odd are therefore  $[1]_2$ . If we look at *division* by 3, we can have **3** possibilities:  $3k [0]_3$ ,  $3k+1 [1]_3$  and  $3k+2 [2]_3$ . These are the integers of modulo 3,  $\mathbf{Z}_3 = \{0,1,2\}$ . The *addition* and *multiplication* tables for these are as shown below.

$+_3$	[0]	[1]	[2]
[0]	[0]	[1]	[2]
[1]	[1]	[2]	[0]
[2]	[1]	[0]	[1]

$\times_3$	[0]	[1]	[2]
[0]	[0]	[0]	[0]
[1]	[0]	[1]	[2]
[2]	[0]	[2]	[1]

Now consider the case of division by 4. We have  $4k [0]_4$ ,  $4k+1 [1]_4$ ,  $4k+2 [2]_4$  and  $4k+3 [3]_4$ . So  $\mathbf{Z}_4 = \{0,1,2,3\}$ . Now, looking at the *tables* below, we can answer the question: squares (in **red**) can have remainder 0 or 1. Adding two square numbers i.e.  $0+0$ ,  $1+0$ ,  $0+1$  or  $1+1$ , gives the **blue answers**, for which you cannot have remainder 3. So the statement is *correct*.

$+_4$	[0]	[1]	[2]	[3]
[0]	[0]	[1]	[2]	[3]
[1]	[1]	[2]	[3]	[0]
[2]	[2]	[3]	[0]	[1]
[3]	[3]	[0]	[1]	[2]

$\times_4$	[0]	[1]	[2]	[3]
[0]	[0]	[0]	[0]	[0]
[1]	[0]	[1]	[2]	[3]
[2]	[0]	[2]	[0]	[2]
[3]	[0]	[3]	[2]	[1]

$\times_6$	[0]	[1]	[2]	[3]	[4]	[5]
[0]	[0]	[0]	[0]	[0]	[0]	[0]
[1]	[0]	[1]	[2]	[3]	[4]	[5]
[2]	[0]	[2]	[4]	[0]	[2]	[4]
[3]	[0]	[3]	[0]	[3]	[0]	[3]
[4]	[0]	[4]	[2]	[0]	[4]	[2]
[5]	[0]	[5]	[4]	[3]	[2]	[1]

## Modular Arithmetic

**Suppose** we have  $ax = b$  (where  $a$  &  $b$  are integers). This has an *integer* solution iff  $a|b$ . Weaker question: if in addition to  $a$  &  $b$ , we have an integer  $n$  given to us, we can then ask if there is an integer  $x$  such that  $ax$  and  $b$  give the same *remainder* on division by  $n$ . **Simple** example:  $n = 4$ ,  $a = 3$ ,  $b = 13$ . Look for those integers  $x$  such that  $3x$  and  $13$  give the same remainder on division by 4.

**Definition:** given integers  $a$  and  $b$  and a +ve integer  $n$ , we say that  $a$  &  $b$  are **congruent modulo  $n$**  if  $a$  and  $b$  have the *same remainder* on division by  $n$ . Notes: (a) if  $a$  and  $b$  have the same remainder on division by  $n$ , then  $a = q_1n+r$ ;  $b = q_2n+r$ . But then  $a-b = (q_1-q_2)n$ , so  $a-b$  is divisible by  $n$ . Also, (b) if  $a-b$  is divisible by  $n$ , then  $a = b+ns = q_2n+r_2 + ns = (q_2+s)n + r_2$ . **So** if  $a = q_1n+r_1$  and  $a \leq r_1 < n$ , we must have  $r_1 = r_2$  by the *uniqueness* clauses of the **division** algorithm.

We have proved a Lemma:  $a$  and  $b$  are *congruent mod  $n$*  iff  $a-b$  is divisible by  $n$ . Notation: write  $a \equiv b \pmod{n}$  (if  $a$  is **congruent** to  $b \pmod{n}$ ). This means that the earlier problem was to solve  $ax \equiv b \pmod{n}$ . Example:  $62 \equiv -234 \pmod{4}$ . *Interpretation:*  $62 = 4 \times 15 + 2$  and  $-234 = -59 \times 4 + 2$ . OR,  $62 - (-234) = 296$  which is **divisible** by 4.

Given  $n$  and any *integer*  $a$ , there is a  $b \in \{0, 1, \dots, n-1\}$  such that  $a \equiv b \pmod{n}$ . For example,  $13 \equiv 1 \pmod{4}$ . Notation: If  $a$  is an *integer*,  $[a]_n = \{b \mid a \equiv b \pmod{n}\}$  (The congruence class mod  $n$  of the integer  $a$ ).  $\mathbf{Z}_n = \{[0]_n, [1]_n, \dots, [n-1]_n\}$ . We often *abuse* notations and write  $\mathbf{Z}_n = \{0, 1, \dots, n-1\}$  if there is no risk of confusion.

We want to solve *linear congruences* such as  $3x \equiv 13 \pmod{4}$  (\*). Suppose  $x = \alpha$  is a solution. Then  $3\alpha - 13 = 4k$  for some *integer*  $k$ . Now assume that  $\beta = \alpha \pmod{n}$ , and we **claim** that  $\beta$  is also a solution of (\*). *Because*  $\beta - \alpha = 4l$  for some *integer*  $l$ , then  $\beta = \alpha + 4l$ ,  $3\beta - 13 = 3\alpha + (4 \times 3l) - 13$  (*multiplying by 4, taking 13 away*);  $3\beta - 13 = 3\alpha - 13 + 4(3l)$ ;  $3\beta - 13 = 4k + 4(3l)$ ;  $3\beta - 13 = 4(k+3l)$ . So  $3\beta = 4(k+3l) + 13$ ;  $3\beta \equiv 13 \pmod{4}$ .

On **generalising**, we have a *Lemma*: Given an integer  $n$  and a solution  $\alpha$  of  $ax \equiv b \pmod{n}$ , then any  $\beta \in [\alpha]_n$  is **also** a solution of this *linear* congruence.

### Assignment 3

(Q1): Find all the **solutions** of the equations: (i)  $z^5 - z^4 + z^3 - z^2 + z - 1 = 0$ ; (ii)  $x^3 + 2 + \frac{1}{z^3} = 0$ .  
(A1): (i) This is a G.P. with  $a = -1$  and common ratio  $-z$ , so this is  $(z^6 - 1)/(z + 1)$ . For this to be *valid*, we must have  $z \neq -1$  (Putting  $z = -1$  in  $p(z)$  gives  $-6$ , which is not 0, so we know  $z = -1$  is **not** a solution to  $p(z) = 0$ ).

If  $p(z) = 0$ , then  $z^6 - 1 = 0$  and  $z \neq -1$ , i.e.  $z^6 = 1$ . So we *roll out* the algorithm for solving  $z^n = b$ . Converting 1 to polar form gives  $1 = 1(\cos 0 + i \sin 0)$ . Put  $z = r(\cos \theta + i \sin \theta)$  to get  $z^6 = 1$ ; this implies that  $r = 1$  and  $6\theta = 2k\pi$  (Here you should *break up the reasoning* and explain a bit more as before i.e.  $\theta_k = 2k\pi/6$ ).

We **expect** 6 solutions to  $z^6 = 1$ , but we know that one of these ( $z = -1$ ) is not a solution of  $p(z) = 0$ , giving the 5 that we want for the equation. Now set  $z_k = \cos\theta_k + i\sin\theta_k$ . ( $r = 1$ ):  $k = 0$  gives  $z_0 = 1$ .  $k = 1$  gives  $z_1 = \cos^{\pi/3} + i\sin^{\pi/3} = \frac{1}{2} + i\frac{\sqrt{3}}{2}$  (Note: *always* put in ‘a+ib’ form if it is one of the (few) polar forms that has a nice expression).

$k = 2$  gives  $z_2 = \cos^{2\pi/3} + i\sin^{2\pi/3} = -\frac{1}{2} + i\frac{\sqrt{3}}{2}$ .  $k = 3$  gives  $z_3 = -1$  (**not** a solution of  $p(z) = 0$ ). ( $k = 4$  — argument *beyond*  $\pi$ ).  $k = -1$  gives  $z_{-1} = \frac{1}{2} - i\frac{\sqrt{3}}{2}$ .  $k = -2$  gives  $z_{-2} = -\frac{1}{2} - i\frac{\sqrt{3}}{2}$ . So *therefore* the solutions are  $1, \frac{1}{2} \pm i\frac{\sqrt{3}}{2}, -\frac{1}{2} \pm i\frac{\sqrt{3}}{2}$ .

(ii)  $z^3 + 2 + \frac{1}{z^3} = 0$ . So  $z^6 + 2z^3 + 1 = 0$  — should get 6 *solutions*.  $(z^3 + 1)^2 = 0$ . So  $z^3 = -1$  (twice). Two methods here: the **algorithm** as before, or note that  $z = -1$  IS a solution, so  $z^3 + 1 = (z + 1)(\text{something!})$ . In fact,  $z^3 + 1 = (z^2 - z + 1)(z + 1)$  by long division. If  $z^3 + 1 = 0$ , either  $z + 1 = 0$  or  $z^2 - z + 1 = 0$ , so  $z = \frac{1}{2} \pm \sqrt{\frac{1-4}{2}} = \frac{1}{2} \pm i\frac{\sqrt{3}}{2}$ . The *solutions* are thus  $-1, \frac{1}{2} \pm i\frac{\sqrt{3}}{2}$  (each counted **twice**).

Each factor occurs twice. This is a *bit like noting that*  $(x^2 + 2x + 1) = 0$  has  $-1$  twice as its solution. The curve touches the x-axis. The fact that the solution occurs with a **multiplicity** greater than 1 is very important for the *properties* of the function  $\frac{1}{z^3}(z^6 + 2z^3 + 1)$  when considered in **complex** calculus.

(Q2): Solve the **linear** equations  $(2+i)x + (1-i)y + iz = 1$ ;  $(4+2i)x + (2-2i)y + x = -1$ . (A2): Solve this using **Gaussian** elimination in a matrix. The only place where you have to be *careful* is when dividing through by complex numbers. We have 2 equations in 3 unknowns so a **parameter** has to be introduced into the solutions.

(Q3): Find the *image* of the circle  $\{z \mid |z-2| = 1\}$  under the function  $f: \mathbf{C} \rightarrow \mathbf{C}$  given by  $f(z) = \frac{z+1}{2z+3}$ . (A3): Set  $w = f(z) = \frac{z+1}{2z+3}$ . Then  $2wz + 3w = z + 1$ ;  $z(2w-1) = 1-3w$ ;  $z = \frac{1-3w}{2w-1}$ . As  $|z-2| = 1$ , we have  $|\frac{1-3w}{2w-1} - 2| = 1$  so that  $|1-3w-4w+2| = |2w-1|$ , i.e.  $|7w-3| = |2w-1|$  (---(a)). For **convenience**, we have written  $|-a| = |a|$  to write  $|3-7w|$  as  $|7w-3|$ : this is *easier* to handle.

Equation (a) gives  $(7u-3)^2 + 49v^2 = (2u-1)^2 + 4v^2$ ;  $49u^2 - 42u + 9 + 49v^2 = 4u^2 - 4u + 1 + 4v^2$ ;  $45u^2 - 38u + 8 + 45v^2 = 0$ ;  $u^2 - \frac{38}{45}u + \frac{8}{45} + v^2 = 0$ ;  $(u - \frac{19}{45})^2 - (\frac{19}{45})^2 + \frac{8}{45} + v^2 = 0$ ;  $(u - \frac{19}{45})^2 + v^2 = 19^2 - \frac{8 \times 45}{(45)^2} = \frac{361 - 360}{45^2} = (\frac{1}{45})^2$ , i.e. the *image* is a circle with centre  $\frac{19}{45}$ ; radius  $\frac{1}{45}$ . Remember to **always compare** with  $(x-a)^2 + (y-b)^2 = r^2$ : a circle with centre  $(a,b)$  and radius  $r$ ; or in *complex* number terms, centre  $a+ib$  and radius  $r$ .

## Tutorial Questions on Modular Arithmetic

In **modular** arithmetic, we fix  $n > 1$ , the modulus. Then we do all *operations* of arithmetic ‘modulo  $n$ ’ in the following sense: when we add or multiply 2 numbers, we record only the **remainder** on division by  $n$ . Example: for  $n = 6$ , we can add ‘mod 6’ so that  $3+5$  is *equivalent* to  $2 \pmod{6}$ . **Multiplying** mod 6 gives for instance  $3 \times 5 \equiv 3 \pmod{6}$ .

A number ‘ $a$ ’ has an inverse mod  $n$  if there’s **another** number  $b$  so that  $a \times b \equiv 1 \pmod{n}$ . The set of *numbers* between 0 and  $n-1$  (inclusive) is **denoted** by  $\mathbf{Z}_n$ , and will always be *thought* of with ‘arithmetic mod  $n$ ’ as its structure (it is another ring).

Q: Write down the **numbers** in  $\mathbf{Z}_{30}$  that have an *inverse* (modulo 30). Without working formally, try to guess the inverse of each of these elements. A: We want two **numbers** in  $\mathbf{Z}_{30}$  which multiply to make 31, 61, 91, 121,... etc., i.e. have remainder 1 on division by 30. These all numbers all end with a 1 so are **odd**. So all even numbers are *excluded*.

*Multiples* of 5 are excluded — they do not end in 1. By trial and error, we get the following:  $1 \times 1 = 1$  so  $1^{-1} \equiv 1 \pmod{30}$ .  $11 \times 11 = 121 \equiv 1 \pmod{30}$ .  $19 \times 19 = 361 = 12 \times 30 + 1 \equiv 1 \pmod{30}$ .  $29 \times 29 = 841 = 30 \times 28 + 1$ .  $7 \times 13 = 91 = 3 \times 30 + 1$ . And  $17 \times 23 = 391 = 13 \times 30 + 1$ . So the *elements* and their inverses are shown in the table below: (notice the **patterns**).

<i>Element</i>	1	7	11	13	17	19	23	29
<i>Inverse</i>	1	13	11	7	23	19	17	29

Q: Find the **inverse** of each element of  $\mathbf{Z}_{34}$  that has one, using, if *necessary*, Euclid's algorithm: given a, find  $\gcd(a, 34)$  as  $ar + 34b$ . Now reduce mod 34. Sometimes this will be 1. **When** does this happen? A: Use the *trial and error* method shown above. But also note that only numbers coprime to 34 will have **inverses**.

<i>Element</i>	1	3	5	7	11	13	15	19	21	23	27	29	31	33
<i>Inverse</i>	1	23	7	5	31					3	29	27	11	33

**23rd April 1999**

**Solve**  $3x \equiv 13 \pmod{4}$ . If there *is* a solution, then there will be one in  $\mathbf{Z}_4 = \{0,1,2,3\}$ . Try them in turn!  $13 \equiv 1 \pmod{4}$ . So we **want**  $3x \equiv 1 \pmod{4}$ . For  $x = 3$ ,  $3x \pmod{4}$  is 1, so this is our *solution*. The solution set of the *congruence* is thus  $[3]_4 = \{4k+3 \mid k \in \mathbf{Z}\} = 3, 7, 11, 15, 19, \dots, -1, -5, \dots$  Good! But try this **method** with  $3x \equiv 13 \pmod{1029485}$ !

Rethink: look at *arithmetic* mod n. We have seen arithmetic mod 30 and mod 34 before: had  $a+b \pmod{n}$  (a, b integers) e.g.  $16 + 19 \equiv 1 \pmod{34}$ ;  $ab \pmod{n}$ :  $16 \times 19 \equiv 16 \pmod{32}$ . Inverses mod n: In  $\mathbf{Z}_5$ ,  $[3]_5^{-1} = [2]_5$  or  $3^{-1} \equiv 2 \pmod{5}$ . No **fractions** needed! We could solve equations mod n:  $3x+5 \equiv 7 \pmod{8}$ ;  $3x+5 = 7 \in \mathbf{Z}_8$ .

In  $\mathbf{Z}_8$ ,  $3x+5 = 7$ ;  $3x = 2$ . *Multiplying* by  $3^{-1}$  (i.e. by 3 itself),  $x \equiv 6$  in  $\mathbf{Z}_8$  (or  $x = [6]_8$ ). Check:  $(3 \times 6) + 5 = 23$  giving **remainder** 7 on division by 8. Which *elements* of  $\mathbf{Z}_n$  have inverses? If  $ab \equiv 1 \pmod{n}$ , then  $ab = 1 + kn$  for some **integer** k, or  $1 = ab + (-k)n$ . This will be possible iff  $\gcd(a,n) = 1$  (by *Euclid's* algorithm). This also tells us how to find b. So a has an inverse mod n iff a and n are coprime **and** we can thus calculate  $a^{-1} \pmod{n}$ .

**Theorem.** In  $\mathbf{Z}_n$ , the elements  $[a]_n$  which have inverses in  $\mathbf{Z}_n$  correspond exactly to those integers a ( $1 \leq a \leq n-1$ ) coprime to n. **Corollary:** If n is a *prime* number, then every  $[a]_n$  other than  $[0]_n$  has an inverse in  $\mathbf{Z}_n$ . In fact,  $\mathbf{Z}_n$  is a field if n is *prime*.

## Solving Linear Congruences

**Result:** The linear congruence  $ax \equiv b \pmod{n}$  has solutions iff  $d \mid b$ , where  $d = \gcd(a, n)$ . If d does divide b, then there are **exactly** d solutions up to congruence mod n; these *solutions* are all congruent mod  $n/d$ .

**Example:** Solve  $117x \equiv 18 \pmod{297}$  (---(1)). 1st step: **Calculate**  $\gcd(a,n)$  in the form  $d = ar+bn$ . Using the *matrix* method, this is  $9 = \gcd(117,297) = 2 \times 297 - 5 \times 117$  (---(2)). 2nd step: Check if  $d \mid$  right hand side i.e. does  $9 \mid 18$ ? Yes! So there are **9** solutions in  $\mathbf{Z}_{297}$ , and they will be *congruent* to each other mod  $297/9 = 33$ .

3rd step: Divide (1) **through** by  $d$  giving  $13x \equiv 2 \pmod{33}$  (---(3)). Now  $\gcd(13,33) = 1 = 2 \times 33 - 5 \times 13$  (Dividing (2) by 9). So  $[13]^{-1} = [-5]_{33} = [28]_{33}$ . 4th step: **Multiply** (3) through by  $[13]^{-1}$  i.e. by  $[-5]$ . So  $x \equiv -5 \times 13x \equiv -10 \equiv 23 \pmod{33}$ . Check:  $23 \times 13 \equiv \dots \equiv 2 \pmod{33}$ . The *solutions* are 23, 56, 89, 122, 155, 188, 221, 254, 287.

26th April 1999

### Another Example

Solve the **linear** congruence  $432x \equiv 12 \pmod{546}$ . (---(1)). By the *matrix* method,  $\gcd(432, 546) = 6 = 19 \times 546 - 24 \times 432$  (---(2)). Note:  $6 \mid 12$  so there will be **6** solutions mod 546. Divide (1) by 6 to give  $72x \equiv 2 \pmod{91}$  (---(3)). Now divide (2) by 6 to give  $1 = 19 \times 91 - 24 \times 72$ . So  $[72]^{-1} = [-24]$  in  $\mathbf{Z}_{546}$ . ( $-24 \equiv 67 \pmod{91}$ ). **Multiplying** (3) through by 67 (or by  $-24$ ) gives  $x \equiv (-24) \times 72x \equiv -58 \equiv 43 \pmod{91}$ , or  $x \equiv (67) \times (72)x \equiv 2 \times 67 = 134 \equiv 43 \pmod{91}$ . The solutions of the *original* linear congruence are  $\{43, 134, 225, 316, 407, 498\}$ . Note: if  $d$  does **not** divide the R.H.S., there are no solutions e.g.  $2x \equiv 3 \pmod{8}$  has no solutions. Always **check** your solutions.

### Assignment Notes

$ax \equiv b \pmod{n}$  is interpreted as **saying** that  $ax-b$  is exactly divisible by  $n$ . For example,  $2x \equiv 1 \pmod{4}$  has no *solutions* since  $2x-1$  is never divisible by 4. On the other hand,  $2x \equiv 1 \pmod{5}$  has an infinite number of solutions. For instance, 3, 8, 13, 18, ... are all solutions of the congruence, but note however that any two of these differ by a multiple of 5. We solve a *congruence* modulo  $n$  by listing all its solutions in  $\mathbf{Z}_n$  which is shorthand for the *set*  $\{0, 1, \dots, n-1\}$ . Method is as follows:

Write  $\gcd(a,n)$  (related to  $ax \equiv b \pmod{n}$ ) in the **form**  $d = as+nt$ . If  $d$  does not divide  $b$ , **STOP**, no solutions. If it does, *divide* everything in the **original** equation by  $d$ . There will be  $d$  solutions in  $\mathbf{Z}_n$ . Take the new *equation*, which has the form  $a'x \equiv b' \pmod{n'}$ . Now  $\gcd(a',n') = 1$ . Note that  $a's \equiv 1 \pmod{n}$ . Now multiply the new equation through by  $s$ , to get  $sa'x \equiv sb' \pmod{n'}$ . But  $x \equiv sa'x \pmod{n'}$ , so this is  $x \equiv sb' \pmod{n'}$ . This gives **1 solution** mod  $n'$  to which we add *multiples* of  $n'$  to this solution until we have all  $d$  solutions in  $\mathbf{Z}_n$ .

### Applications of Modular Arithmetic

Method for checking for **integer** solutions, e.g. does  $x^4+3x^2+x+2$  have any *integer* roots? Suppose that  $k$  is an integer root, then  $k^4+3k^2+k+2 = 0$ . **Reducing** mod 2,  $[k^4]_2 + [3k^2]_2 + [k]_2 + [2]_2 = [0]_2$ , i.e.  $[k]_2^4 + [k]_2^2 + [k]_2 = [0]_2 \in \mathbf{Z}_2 = \{0,1\}$ . Try  $[k]_2 = [0]_2$ , which could happen. Now try  $[k]_2 = [1]_2$ , which gives  $[1]_2^4 + [1]_2^2 + [1]_2 = [3]_2 = [1]_2 \neq [0]_2$ . So if an integer solution exists, it must be **even**.

Reducing *mod* 3,  $[k]_3^4 + [k]_3 + [2]_3 = [0]_3 \in \mathbf{Z}_3 = \{0,1,2\}$ .  $[k]_3 = [0]_3$  — *no* solutions; similarly for  $[k]_3 = [1]_3$  and  $[k]_3 = [2]_3$ . No solution mod 3, so no **integer** solution.

## Polynomial Congruences (Quadratics)

What numbers **satisfy** an equation of the form  $x^2 \equiv n \pmod{p}$  ( $p$  prime)? *Example:*  $p = 11$ . The numbers 2, 6, 7, 8, 10 do not have **square roots** in  $\mathbf{Z}_{11}$ . How many *squares* are there in  $\mathbf{Z}_p$ : if  $p$  is an odd prime, then there are  $(p-1)/2$  squares — why?

28th April 1999

## Coding & Decoding

Modular arithmetic is useful for **codes**. We shall summarise about the Euler phi-function. Given any positive *integer*  $n$ ,  $\phi(n)$  denotes the number of integers between 1 and  $n$  inclusive which are *coprime* to  $n$ . If  $a$  and  $b$  are coprime, then  $\phi(ab) = \phi(a)\phi(b)$ . If  $p$  is a **prime** number and  $n$  is a positive integer, then  $\phi(p^n) = p^n - p^{n-1}$ . In particular,  $\phi(p) = p-1$ .

RSA Codes. Pick two (large) **primes**  $p$  &  $q$ . For  $n = pq$ , we have  $\phi(n) = (p-1)(q-1)$ . Choose a number 'a' coprime to  $\phi(n)$ . Write 1 as a *linear* combination of  $a$  and  $\phi(n)$ , namely  $ax + \phi(n)y = 1$ . Note, in particular, that  $x$  is the **inverse** of 'a' modulo  $\phi(n)$ . You may now "*publish*" the pair of numbers  $(n, a)$ .

To **encode** a message, first assign a letter to some number e.g.  $a = 01$ ,  $b = 02$ , ...,  $z = 26$ , etc. Then break your digitised message into blocks **less** than the number of digits in either  $p$  or  $q$ . Now encode each block  $B$  by calculating  $B^a$  modulo  $n$ . Now send the sequence of encoded blocks with the beginning of each block *clearly* defined or **marked** in some way.

Decoding. When receiving a message, break it into blocks. To decode a *block*  $M$ , calculate  $M^x \pmod{n}$ . The result is the *original* block  $B$  of the message. This uses a result known as Euler's theorem that states that if  $b$  is **coprime** to  $n$ , then  $b^{\phi(n)} \equiv 1 \pmod{n}$ .

Q: 41 58 is received *encrypted*, with  $n = 1679 = 73 \times 23$  and  $a = 679$ . What was the original message? A: As  $n = 73 \times 23$ ,  $\phi(n) = 72 \times 22 = 1584$ . Using Euclid's algorithm,  $1 = 7 \times 679 - 3 \times 1584$ . So  $x = 7$ . Taking the **first** block, 41, we raise it to the power 7 and reduce modulo 1679. Using *Quattro Pro*,  $41^7 \equiv 328 \pmod{1679}$  whilst  $57^7 \equiv 775 \pmod{1679}$ . So the *decoded* message was 328 775.

Q: **Decode** the following: 077 with  $n = 1189 = 29 \times 41$  and  $a = 59$ . A:  $\gcd(59, 1120) = 1$  (in the *usual* way)  $= 1 = -1 \times 1120 + 19 \times 59$ . So  $x = 19$ . Now take the block 077 to the power 19 and reduce mod 1189. Note:  $a \equiv b \pmod{c}$  means that  $a-b$  is divisible by  $c$ . We can work out **manually** that  $77^2 \equiv 1173 \pmod{1189}$  and  $77^4 \equiv 256 \pmod{1189}$ . Then squaring, we obtain  $(77^4)^4 = ? \pmod{1189}$ . To get  $?$ , **square** 256, divide by 1189 and see what integer you obtain (e.g. 55.44343).

Then do 55  $\times 1189$ , take away 256 squared, and you get the *remainder* — this is the ' $?$ '. Then, do  $77^{19} = (77^{16})^3$ . To get  $?$  here, you get the  $b$  coefficient of  $77^{16} \equiv b \pmod{1189}$  and multiply it with the corresponding *coefficient* for  $77^3$ , and then follow the procedure above (but here "taking away 256<sup>2</sup>" is replaced by taking away the product of the  $b$  coefficients).

30th April 1999

## Fermat's Little Theorem

Examine the **binomial** expansion of  $(a+b)^p$  (where  $p$  is a prime). The *general* term is of the form  ${}^pC_r a^r b^{p-r}$ . If  $r \neq 0$  and  $r \neq p$ , then  ${}^pC_r = \frac{p \cdot (p-1)!}{r!(p-r)!}$ . But  $p$  is prime, so *none* of the factors in the denominator can divide  $p$  (nontrivially). So  $p \nmid {}^pC_r$  if  $r \neq 0$  and  $r \neq p$ . We **thus** have  $(a+b)^p \equiv a^p + b^p \pmod p$  for any *integers*  $a$  and  $b$ .

Notice that  $0^p \equiv 0 \pmod p$  and  $1^p \equiv 1 \pmod p$ . Using  $(a+1)^p \equiv a^p + 1^p = a^p + 1 \pmod p$ , we prove by *induction* that  $a^p \equiv a \pmod p \forall$  integers  $a$ . **Proposition:** For any  $a \in \mathbf{Z}_p$ ,  $a^p \equiv a \pmod p$ . Now suppose that  $a \neq 0$ , so  $a \in \{1, \dots, p-1\}$ . Then  $\gcd(a,p) = 1$  and  $a$  is **invertible** mod  $p$ .

**Corollary** (Fermat's Little Theorem). For any *non zero*  $a$  ( $a \in \mathbf{Z}_p$ ),  $a^{p-1} \equiv 1 \pmod p$ . We thus have that  $x^{p-1} - 1 \equiv (x-1)(x-2)\dots(x-p+1) \pmod p$ . **Corollary:** For any prime  $p$ , the *coefficients* of the polynomial  $(x^{p-1} - 1) - \prod_{r=1}^{p-1} (x-r)$  are all *divisible* by  $p$  (Note:  $\Sigma$  is *add*,  $\Pi$  is *multiply*). **Proof:** Reduce the polynomial mod  $p$  to get zero! For example,  $p = 5$  gives  $(x-1)(x-2)(x-3)(x-4) = x^4 - 10x^3 + 35x^2 - 50x + 24$ : the coefficients are all *divisible* by 5 except the first and the last.

**Theorem:** *Wilson's* Theorem. For any prime  $p$ ,  $(p-1)! \equiv -1 \pmod p$ . Proof: Put  $x = 0$  in the above polynomial.

## Euler's $\phi$ Function

Let  $n$  be a **positive** integer,  $n \geq 2$ . **Definition:**  $\phi(n) =$  number of  $r$ ,  $1 \leq r \leq n$ , such that  $\gcd(r,n) = 1$ .  $\phi$  is called Euler's phi-function.

5th May 1999

## Tutorial: When does an Equation have Integer Solutions?

There are methods of **factorisation** of polynomials provided that the coefficients are taken from a field. We know of *various* examples of fields:  $\mathbf{R}$ ,  $\mathbf{C}$  and  $\mathbf{Z}_p$ . Consider the equation  $x^2 + 1 = 0$ . We know it does *not* have integer roots: if it did, then there would be some  $k$  such that  $k^2 + 1 \equiv 0 \pmod n$  for *any* integer  $n$ .

Show that the **equation**  $x^3 - x^2 + x + 1 = 0$  has no integer solutions. A: Consider  $x^3 + x^2 + x + 1 \equiv 0 \pmod 2$ . Consider  $x$  to be even (so we have  $[0]_2$ ). So  $[0]_2^3 - [0]_2^2 + [0]_2 + [1]_2 \equiv 0 \pmod 2$ ;  $[0]_2 - [0]_2 + [0]_2 + [1]_2 = [0]_2$ ;  $[1]_2 \neq [0]_2$ . Now **consider**  $x$  to be odd ( $[1]_2$ ). So  $[1]_2^3 - [1]_2^2 + [1]_2 + [1]_2 \equiv [0]_2$ ;  $[1]_2 - [1]_2 + [1]_2 + [1]_2 = [0]_2$ ;  $[0]_2 = [0]_2$ . So there **could** be an *odd* solution.

Now *consider*  $\mathbf{Z}_3$ . For  $x = [0]_3$ ,  $[0]_3^3 - [0]_3^2 + [0]_3 + [1]_3 \equiv [0]_3$ ;  $[0]_3 - [0]_3 + [0]_3 + [1]_3 \neq [0]_3$ . Now consider  $x = [1]_3$ .  $[1]_3^3 - [1]_3^2 + [1]_3 + [1]_3 = [0]_3$ ;  $[1]_3 - [1]_3 + [2]_3 \neq [0]_3$ . And for  $x = [2]_3$ ,  $[2]_3^3 - [2]_3^2 + [2]_3 + [1]_3 = [0]_3$ ;  $[2]_3 - [1]_3 + [2]_3 + [1]_3 = [0]_3$ ;  $[1]_3 \neq [0]_3$ . So we have **proved** that there are no *integer* solutions.

## Euler's $\phi$ Function

Let  $n$  be a **positive** integer  $\geq 2$ . Definition:  $\phi(n) =$  number of  $r$ ,  $1 \leq r \leq n-1$ , such that  $\gcd(r, n) = 1$ .  $\phi$  is Euler's *phi-function*. Examples:  $\phi(5) = 4$  since 1, 2, 3 and 4 are **coprime** to 5.  $\phi(23) = 22$ . In general,  $\phi(p) = p-1$ .  $\phi(9) = ? = 6$  because in the numbers from 1 to 8, 3 and 6 are not coprime to 9, so we have 6 coprime numbers.  $\phi(p^2) = 1, 2, \dots, p, \dots, 2p, \dots, p^2-1$ . These *multiples* of  $p$  are not coprime to  $p^2$ , so we must take them **out**. So  $\phi(p^2) = (p^2-1)-(p-1) = p^2-p$ .

**Theorem:**  $\phi(p^n) = p^n - p^{n-1}$ . *Proof:* Count carefully! The set  $\{1, \dots, p^n-1\}$  has  $p^n-1$  elements.  $\{p, \dots, p^n-p\}$  has  $p^{n-1}-1$  elements. So  $\{1, \dots, p^n-1\} \setminus \{p, \dots, p^n-p\}$  is the set of *numbers* coprime to  $p^n$ . Theorem: if  $\gcd(a, b) = 1$ , then  $\phi(ab) = \phi(a)\phi(b)$ . From this and the *prime* decomposition theorem, we can get  $\phi(m)$  for any  $m$ , e.g.  $\phi(100) = \phi(2^2)\phi(5^2) = (2^2-2).(5^2-5) = 2.20 = 40$ .

**Another** proof of FLT.  $G_p =$  set of invertible *elements* mod  $p = \{[1]_p, \dots, [p-1]_p\}$ . If  $a$  is not congruent to 0 mod  $p$ , then form the set  $aG_p = \{ab \mid b \in G_p\}$  reduced mod  $p = \{[a_1]_p[a_2]_p \dots [(p-1)]_p\} \subseteq G_p$ . Are there *repetitions* in this list? No, because  $[a_1b_1] = [a_1b_2]$  implies that  $b_1 = b_2$  and that  $[a]^{-1}$  exists. ( $a_1b_1 \equiv a_1b_2 \pmod{p} \Rightarrow b_1 \equiv b_2 \pmod{p}$ ).

Thus  $a.G_p$  has exactly  $p-1$  elements and  $a.G_p = G_p$ . Next, multiply all the **elements** in  $G_p$  together and reduce mod  $p$ .  $[N]_p = [1]_p[2]_p \dots [p-1]_p \in G_p$ . But  $[N]_p$  also equals  $[a]_p[1]_p[a]_p[2]_p \dots [a]_p[p-1]_p$  since  $a.G_p = G_p$ . So  $[N]_p = [a]^{p-1}_p[N]_p$ . But  $[N] \in G_p$ , so it is invertible. Thus we can *divide* by  $[N]$  to get  $[a]^{p-1}_p = [1]_p$ , i.e.  $a^{p-1} \equiv 1 \pmod{p}$ .

Really, this proof **hinges** on the fact that  $[a]$  has an inverse mod  $p$ . *Euler's* Theorem: Let  $n \in \mathbf{Z}$ ,  $n \geq 2$ ; and let  $a \in \mathbf{Z}$ ,  $\gcd(a, n) = 1$ . Then  $a^{\phi(n)} \equiv 1 \pmod{n}$ . **Proof:** Let  $G_n$  be the set of invertible elements mod  $n$ ,  $G_n = \{b \mid \exists c \text{ with } bc \equiv 1 \pmod{n}\}$ . ( $1 \leq b \leq n-1$ ).  $G_n$  has  $\phi(n)$  elements because  $b$  is *invertible* mod  $n$  iff  $\gcd(b, n) = 1$ .

**Claim:** If  $\gcd(a, n) = 1$ , then  $a.G_n = G_n$  (as before). Form  $[N] =$  the *product* of the elements in  $G_p =$  the product of the elements in  $a.G_p = [a]^{\phi(n)}[N]$ . Now  $[N] \in G_n$ , so  $[N]^{-1}$  exists and therefore  $[a]^{\phi(n)} = [1]$ . So  $a^{\phi(n)} \equiv 1 \pmod{n}$ . *Example:*  $n = 8$  gives  $\phi(n) = 4 (= 2^3-2^2)$ .  $G_8 = \{1, 3, 5, 7\}$ . Look at  $5^{\phi(8)} = 5^4 = 625 = (8 \times 78) + 1 \equiv 1 \pmod{8}$ . Now go to *coding & decoding*.

10th May 1999

## Past Paper

Q: Find  $\gcd(3024, 4023)$  in the **form**  $ar+bs$ . Then find  $\text{lcm}(3024, 4023)$ . A: Remember to write  $\gcd(a, b)$  in *matrix* form as  $\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} a \\ b \end{pmatrix}$ . Then after manipulation, e.g. for this question  $\begin{pmatrix} 112 & -149 \\ -3 & 4 \end{pmatrix} \begin{pmatrix} 3024 \\ 4023 \end{pmatrix}$ , we get  $\gcd(3024, 4023) = 27 = -3 \times 4023 + 4 \times 3024$ . And **also**  $112 \times 4023 - 149 \times 3024 = 0$ ;  $112 \times 4023 = 149 \times 3024$ ;  $450576 = 450576$ . So  $\text{lcm}(3024, 4023) = 450576$ . Check: An lcm can be *obtained* by multiplying the two numbers together and dividing through by the gcd.

Q: Write down the **numbers** in  $\mathbf{Z}_{20}$  that have an inverse *modulo* 20. A: Write down the set  $\{1, 2, 3, \dots, 18, 19\}$ . Multiples of 2 and 5 excluded (because  $2 \times 2 \times 5 = 20$ ). We want numbers in  $\mathbf{Z}_{20}$  such that  $\gcd(a, 20) = 1$ . So  $a = \{1, 3, 7, 9, 11, 13, 17, 19\}$ .

Q: Solve the **equation**  $(2+\sqrt{3}i)z = 1+3i$ . A: Find  $(2+\sqrt{3}i)^{-1} = \frac{(2-\sqrt{3}i)}{7}$ . So  $z = (1+3i)\frac{(2-\sqrt{3}i)}{7}$ ; ...,  $z = \frac{(2+3\sqrt{3}) + (6-\sqrt{3}i)}{7}$ .

Q: Find the *remainder* when  $x^4-3x^2+2x-3$  is divided by  $x^2-2$ . A: Use long division. Then write in the **form** original expression = (dividing expression) $\times$ quotient + remainder. So for our *expression*, we write  $x^4-3x^2+2x-3 = (x^2-2)(x^2-1) + (2x-5)$ . Remember to check at the end by substituting in a **simple** value.

$$\begin{array}{r} \frac{x^2 - 1}{x^2-2} \overline{) x^4-3x^2+2x-3} \\ \underline{x^4-2x^2} \phantom{-3} \\ -x^2+2x-3 \\ \underline{-x^2} \phantom{+2} \\ 2x-5 \end{array}$$

Q: Prove by **induction** that  $\sum_{k=1}^n \frac{1}{4k^2-1} = \frac{n}{2n+1}$ . A: First check the case  $n = 1$ , then assume it is true for all  $n$ . Then we look at the *case*  $n+1$ :  $\sum_{k=1}^{n+1} \frac{1}{4k^2-1} = \sum_{k=1}^n \frac{1}{4k^2-1} + \frac{1}{4(n+1)^2-1} = \frac{n}{2n+1} + \frac{1}{4(n+1)^2-1}$  (The shaded bit appears by using the *inductive* hypothesis). We need to manipulate this to give  $\frac{(n+1)}{2(n+1)+1} = \frac{n+1}{2n+3}$ . So *manipulating*,  $\frac{n}{2n+1} + \frac{1}{4(n^2+2n+1)-1} = \frac{n}{2n+1} + \frac{1}{4n^2+8n+4-1} = \frac{n}{2n+1} + \frac{1}{4n^2+8n+3} = \frac{n(4n^2+8n+3)+2n+1}{(2n+1)(4n^2+8n+3)} = \frac{n(2n+3)(2n+1)+2n+1}{(2n+1)(2n+3)(2n+1)} = \frac{(2n+1)(n(2n+3)+1)}{(2n+1)(2n+1)(2n+3)} = \frac{n(2n+3)+1}{(2n+1)(2n+3)} = \frac{2n^2+3n+1}{(2n+1)(2n+3)} = \frac{(2n+1)(n+1)}{(2n+1)(2n+3)} = \frac{n+1}{2n+3}$ . QED.

Q: Prove that  $\sqrt{10}$  is irrational. A: As before, *assume* that  $\sqrt{10} = \frac{a}{b}$ , with the fraction in its lowest form i.e.  $\gcd(a,b) = 1$ . Then  $10 = \frac{a^2}{b^2}$ ;  $10b^2 = a^2$ . So  $a^2$  is *divisible* by 10. Here, break it up into prime factors. Then apply the same argument as before i.e. so  $a^2$  is divisible by 5 and 2; so  $a$  is *divisible* by 2. Therefore,  $a = 2a'$ . Now  $b^2 = (2a')^2$ ;  $10b^2 = 4a'^2$ ;  $b^2 = \frac{4a'^2}{10} = \frac{2a'^2}{5}$ . So  $b^2$  is divisible by 2, *implying that*  $b$  is divisible by 2. But  $a$  &  $b$  cannot **both** be divisible by 2, because  $\gcd(a,b) = 1$  i.e. they are coprime. Thus  $\sqrt{10}$  cannot be *written* as  $\frac{a}{b}$  i.e. it is irrational.

Q: Find the **gcd** of  $p(x)$  and  $q(x)$  in the form  $pr+qs$ , where  $p(x) = x^2-3x+2$  and  $q(x) = x^3+3x^2-6x+2$ . A: Here, think of the **table** on page 1. Applying *long* division to  $p(x)$  and  $q(x)$ , we get  $x^3+3x^2-6x+2 = (x^2-3x+2)(x+6) + (10x-10)$ . The remainder is not zero, so we repeat: dividing  $x^2-3x+2$  by  $10x-10$  to get  $x^2-3x+2 = (10x-10)(\frac{1}{10}x-\frac{1}{5}) + 0$ . Here, the remainder **is** zero, so the gcd is the *remainder* "on the line above" i.e.  $10x-10$ . Now we can write  $10x-10 = 1 \times (x^3+3x^2-6x+2) - (x+6) \times (x^2-3x+2) = 1 \times p(x) - (x+6) \times q(x)$ .

## Assignment 4

Q: Solve the **linear congruence**  $356x \equiv 36 \pmod{468}$  (---(1)). A: First, we calculate  $\gcd(356, 468)$  in the usual way:  $4 = (35 \times 468) - (46 \times 356)$  (---(2)). To check whether the congruence has solutions, we check to see whether 4 **divides** 36. It does, ( $36 = 9 \times 4$ ), so we can divide (1) by 4 to give  $89x \equiv 9 \pmod{117}$  (---(3)).

We now know that *there are 4 solutions* to the linear congruence in  $\mathbf{Z}_{468}$ . Dividing (2) by 4, we obtain  $\gcd(89,117) = 1 = (35 \times 117) - (46 \times 89)$  (---(4)). From (4),  $-46 \times 89 = (-35 \times 117) + 1$ ;  $-46 \times 89 \equiv 1 \pmod{117}$ . So  $[89]^{-1} = [-46]_{117}$ . Multiplying (3) through by  $[89]^{-1}$  i.e. by  $-46$ , we get  $x \equiv (89 \times -46)x \equiv -414 \pmod{117}$ . This gives  $-414$  as a *base* to find solutions in  $\mathbf{Z}_{468}$ .

We add *multiples* of 117 to  $(-414)$  to get the 4 solutions in  $\mathbf{Z}_{468}$ :  $-414 + (4 \times 117) = 54$ ;  $-414 + (5 \times 117) = 171$ ;  $-414 + (6 \times 117) = 288$ ;  $-414 + (7 \times 117) = 405$ . We finish by checking the **validity** of one of the *solutions*: for 54,  $(356 \times 54) - 36$  is exactly divisible by 468, since  $(356 \times 54) - 36 = 19188 = 41 \times 468$ . **Conclusion:** In  $\mathbf{Z}_{468}$ , the 4 solutions to equation (1) are  $x = \{54, 171, 288, 405\}$ .

## Exam Paper: May 1999

### SECTION 1 (Compulsory)

- (1) (a) Find the greatest common divisor of  $a = 1357$  and  $b = 2468$  in the form  $ar + bs$  where  $r$  and  $s$  are integers. Find also the least common multiple of  $a$  and  $b$ . **[5 marks]**
- (b) Prove by induction that  $\sum_{k=1}^n (k-1)k = \frac{(n-1)n(n+1)}{3}$ . **[4 marks]**
- (c) Write down the numbers in  $\mathbf{Z}_{18}$  that have an inverse under multiplication modulo 18. For each, give the corresponding inverse with reasons. **[4 marks]**
- (d) Solve the equation  $(3+i\sqrt{2})z = 1+3i$ . **[4 marks]**
- (e) Find the remainder when  $x^5 + 2x^3 - 2x + 4$  is divided by  $x^2 + 2$ . **[3 marks]**

### SECTION 2 (Answer 2 out of 4 questions)

- (2) (a) Solve the equation  $z^6 = -1$  giving the solutions in the form  $a+ib$ , (do **not** leave them in polar form; you should evaluate the cos and sine terms). **[8 marks]**
- (b) Prove by induction  $\sum_{k=1}^n k.k! = (n+1)! - 1$ . **[7 marks]**
- (3) (a) Prove that there are infinitely many prime numbers. **[7 marks]**
- (b) Find the image of the unit circle  $\{z : |z| = 1\}$  under the function  $f : \check{\mathbf{S}} \rightarrow \check{\mathbf{S}}$  given by  $f(z) = \frac{z-1}{z+2}$ . **[8 marks]**
- (4) Find all solutions in  $\mathbf{Z}_{345}$  of the congruence  $100x \equiv 65 \pmod{345}$ . **[15 marks]**
- (5) Let  $p$  be a prime number. Prove the following:
- (i) For  $r$  in the range  $0 < r < p$ , the binomial coefficient  $\binom{p}{r}$  is divisible by  $p$ ; **[5 marks]**
- (ii) For any integer  $n$ ,  $(n+1)^p \equiv n^p + 1$ , by using the binomial theorem and (i); **[5 marks]**
- (iii) For any integer  $n \geq 0$ ,  $n^p \equiv n \pmod{p}$ , (by induction using (ii)). **[5 marks]**

(Questions done: 1, 3, 4)