

## Chapter 1: The Integers

**Modulo Arithmetic.** *Definition:* Let  $m$  be a fixed positive integer. We define *congruence* ( $\equiv$ ) modulo  $m$  for  $a, b \in \mathbf{Z}$  by  $a \equiv b \pmod{m} \Leftrightarrow m$  divides  $(a-b)$ ; or  $a \equiv b \pmod{m} \Leftrightarrow a = b+rm$  for some  $r \in \mathbf{Z}$ . Notes:  $a \equiv a \pmod{m}$  and  $0 \equiv m \pmod{m}$ . *Examples:*  $2 \equiv 4 \pmod{2}$ ;  $2 \equiv 6 \pmod{2}$ ;  $19 \equiv 5 \pmod{7}$ ;  $-3 \equiv 3 \pmod{3}$ ;  $-3 \equiv -6 \pmod{3}$ ;  $0 \equiv 18 \pmod{6}$ . Note: for a fixed  $m \in \mathbf{Z}^+$ , every  $m \in \mathbf{Z}$  is congruent mod  $m$  to 1 and only 1 of the set  $\mathbf{Z}_m = \{0,1,2,\dots,(m-1)\}$ , e.g.  $-21 \equiv 5 \in \mathbf{Z}_{13}$ .

**Addition & Multiplication.** We can add and multiply in  $\mathbf{Z}_m$  as usual, and then reduce to  $\mathbf{Z}_m$  using *congruence*. This produces a closed system. Example:  $m = 7$ , so  $\mathbf{Z}_7 = \{0,1,2,3,4,5,6\}$ . The *Cayley Tables* are as shown on the right.

+	0	1	2	3	4	5	6
0	0	1	2	3	4	5	6
1	1	2	3	4	5	6	0
2	2	3	4	5	6	0	1
3	3	4	5	6	0	1	2
4	4	5	6	0	1	2	3
5	5	6	0	1	2	3	4
6	6	0	1	2	3	4	5

×	0	1	2	3	4	5	6
0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6
2	0	2	4	6	1	3	5
3	0	3	6	2	5	1	4
4	0	4	1	5	2	6	3
5	0	5	3	1	6	4	2
6	0	6	5	4	3	2	1

Notes: (1) *Addition:* cycling occurs. (2) *Multiplication:* only the non-zero part is significant. Denote by  $\mathbf{Z}_m^*$  the *non-zero* members of  $\mathbf{Z}_m$ . (3) *Symmetry* about the diagonal. (4) **Every** number occurs **only** once in each row & column. (5) We can *solve equations* in  $\mathbf{Z}_7$ , e.g.  $x+6 \equiv 1 \pmod{7}$  gives  $x = 2$ ;  $3x \equiv 5 \pmod{7}$  gives  $x = 4$ . (6) We can **always have**  $ax \equiv 1 \pmod{m}$  ( $a \neq 0$ ) in  $\mathbf{Z}_7$  (i.e.  $a \in \mathbf{Z}_7^*$ ) because each row of the multiplication table contains a 1. We say that “a” has a *multiplicative inverse*  $a^{-1}$ , and that  $\mathbf{Z}_7^*$  forms a multiplicative group. Example:  $m = 4$ , so  $\mathbf{Z}_4 = \{0,1,2,3\}$ . Here, the multiplication table *does not have* a 1 in each row — so we *cannot solve*  $2x \equiv 1 \pmod{4}$ . (Because 4 is **not** a prime number). So  $\mathbf{Z}_m^*$  is a multiplicative group *iff*  $m$  is prime.

+	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

## The Division Properties of the Integers

**Definition:** The g.c.d. of  $a, b \in \mathbf{Z}$ ,  $d = \gcd(a,b)$ , has the following *defining properties*: (1)  $d|a$  and  $d|b$  ( $d$  divides  $a$  &  $b$ ). (2) If  $x|a$  and  $x|b$ , **then**  $x|d$ . (3) For some  $r, s \in \mathbf{Z}$ ,  $d = ar+bs$ . We can find  $d$  by use of the Euclidean Division Algorithm or its **matrix** equivalent, i.e. assuming that  $a < b$ , find  $q$  s.t.  $b = qa+r$  (where  $0 \leq r < a$ ). Then  $\gcd(a,b) = \gcd(a,r)$ , and so on. Further more,  **$b-qa = r$** .

*Example:*  $a = 30$ ,  $b = 171$ . The *algorithm* goes as follows:  $171 = 5 \times 30 + 21$ ;  $30 = 1 \times 21 + 9$ ;  $21 = 2 \times 9 + 3$ ;  $9 = 3 \times 3$ . So  $d = \gcd(171,30) = 3$ . Using the *matrix* method, we reduce  $\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \begin{matrix} | \\ | \end{matrix} \begin{matrix} a \\ b \end{matrix}$  until a value in the *last* column is zero. So we have  $\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \begin{matrix} | \\ | \end{matrix} \begin{matrix} 171 \\ 30 \end{matrix} \sim \begin{pmatrix} 1 & -5 \\ 0 & 1 \end{pmatrix} \begin{matrix} | \\ | \end{matrix} \begin{matrix} 21 \\ 30 \end{matrix}$  ( $R_1 - 5R_2$ );  $\sim \begin{pmatrix} 1 & -5 \\ 0 & 1 \end{pmatrix} \begin{matrix} | \\ | \end{matrix} \begin{matrix} 21 \\ 30 \end{matrix}$  ( $R_2 - R_1$ );  $\sim \begin{pmatrix} 3 & -17 \\ 0 & 1 \end{pmatrix} \begin{matrix} | \\ | \end{matrix} \begin{matrix} 3 \\ 30 \end{matrix}$  ( $R_1 - 2R_2$ );  $\sim \begin{pmatrix} 3 & -17 \\ 0 & 1 \end{pmatrix} \begin{matrix} | \\ | \end{matrix} \begin{matrix} 3 \\ 30 \end{matrix}$  ( $R_2 - 3R_1$ ). Now see that  **$\gcd = 3 = 3 \times 171 - 17 \times 30$** .

**Definition:** The lcm “ $m$ ” of  $a, b \in \mathbf{Z}$  has the following *defining properties*: (i)  $a|m$  and  $b|m$ . (ii) If  $a|x$  and  $b|x$ , then  $m|x$ . (iii)  $ab = \{\text{lcm}(a,b)\} \times \{\text{gcd}(a,b)\}$ . Example:  $\text{lcm}(171,30) = \frac{(30 \times 171)}{3} = 1710$ . Notes. (i)  $\gcd(a,0) = a$  for all  $a \in \mathbf{Z}$  ( $a$  divides 0,  $a \times 0 = 0$ ). (ii) If  $p$  is *prime* and  $a \in \mathbf{Z}$ , with  $a \neq p$ , then  $\gcd(a,p) = 1$ . (iii) For any  $a, b \in \mathbf{Z}$ , if  $\gcd(a,b) = 1$ , we say that  $a$  &  $b$  are *relatively prime*, and so for some  $r, s \in \mathbf{Z}$ , we have  $ar+bs = 1$ .

**Unique Factorisation.** For every positive integer “a”, we can write ‘a’ as a unique expression of a *product* of primes,  $a = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_r^{\alpha_r}$ . If  $a = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_r^{\alpha_r}$  and  $b = p_1^{\beta_1} \dots p_r^{\beta_r}$  (where *some*  $\alpha_i, \beta_i$  may be zero, i.e.  $p_i$  not a factor in **this** case), then  $\gcd(a,b) = p_1^{k_1} \dots p_r^{k_r}$ , where for *each*  $i$ ,  $k_i$  is the **smallest** of the  $\alpha_i, \beta_i$ ; and  $\text{lcm}(a,b) = p_1^{t_1} \dots p_r^{t_r}$ , where for each  $i$ ,  $t_i$  is the **largest** of the  $\alpha_i, \beta_i$ . **Example:**  $a = 135, b = 639$ . Here,  $135 = 3^3 \times 5$ , and  $639 = 3^2 \times 71$ . Now  $135 = 3^3 \times 5 \times 71^0$ , and  $639 = 3^2 \times 5^0 \times 71$ . So  $\gcd(135, 639) = 3^2 \times 5^0 \times 71^0 = 9$ ; and  $\text{lcm}(135, 639) = 3^3 \times 5 \times 71 = 9585$ .

## Implications for Modular Arithmetic

Consider  $\mathbf{Z}_m^* = \{1,2,3,\dots,(m-1)\}$  under *multiplication mod m*. **Definition:** We say that  $a \in \mathbf{Z}_m^*$  is **invertible** with **multiplicative inverse**  $a^{-1}$  if for *some*  $a^{-1} \in \mathbf{Z}_m^*$ ,  $aa^{-1} \equiv a^{-1}a \equiv 1 \pmod{m}$ . **Notes:** (1) If  $a^{-1}$  exists, then it is *unique* to  $a$ . **Proof:** If  $aa_1^{-1} \equiv a_1^{-1}a \equiv 1$ , and  $aa_2^{-1} \equiv a_2^{-1}a \equiv 1$ , then  $a_1^{-1} \equiv a_1^{-1} \times 1 \equiv a_1^{-1}(aa_2^{-1}) \equiv (a_1^{-1}a)a_2^{-1} \equiv 1 \times a_2^{-1} \equiv a_2^{-1}$ . (Use *associativity*). (2)  $a^{-1}$  is **invertible** with inverse  $a$ ,  $(a^{-1})^{-1} = a$ .

(3)  $(ab)^{-1} \equiv b^{-1}a^{-1}$ , provided  $a^{-1}$  and  $b^{-1}$  **exist**. **Proof:**  $(b^{-1}a^{-1})(ab) \equiv b^{-1}(a^{-1}a)b \equiv b^{-1}b \equiv 1 \equiv aa^{-1} \equiv a(bb^{-1})a^{-1} \equiv (ab)(b^{-1}a^{-1})$ . This will be *generalised* when we look at **abstract groups**. **Example:** in  $\mathbf{Z}_7^*$ ,  $3^{-1} = 5$  ( $5^{-1} = 3$ ), and *every* member of  $\mathbf{Z}_7^*$  is invertible, since 1 occurs in *every* row/column of the table. In  $\mathbf{Z}_4^*$ , 1 is invertible ( $1^{-1} = 1$  always);  $3^{-1} = 3$ ; but 2 is **not** invertible.

**Theorem.**  $a \in \mathbf{Z}_m^*$  is *invertible* iff  $\gcd(a,m) = 1$ . (**Relatively prime**). In this case, if  $r$  &  $s$  are s.t.  $ar+ms = 1$ , then  $a^{-1} \equiv r \pmod{m}$  ( $ar \equiv 1 \pmod{m}$ ). **Corollary:** If  $p$  is prime, then *every* member of  $\mathbf{Z}_p^*$  is *invertible* since  $\gcd(a,p) = 1$  for all  $a \in \mathbf{Z}_p^*$ . **Notation:** Put  $U(\mathbf{Z}_m^*) =$  the set of *invertible* elements in  $\mathbf{Z}_m^*$ . If  $m$  is *prime*, then  $U(\mathbf{Z}_m^*) = \mathbf{Z}_m^*$ .

**Example:** Find all *invertible* elements and their inverses in  $\mathbf{Z}_{18}^*$ . Now  $18 = 2 \times 3^2$  is not prime, so any multiple of 2 & 3 will *not* be relatively prime to 18. Therefore,  $U(\mathbf{Z}_{18}^*) = \{1,5,7,11,13,17\}$ . Now find the **inverse** of 5 by the matrix method:  $(\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix} \mid \begin{smallmatrix} 18 \\ 5 \end{smallmatrix}) \sim (\begin{smallmatrix} 1 & 0 \\ 0 & -3 \end{smallmatrix} \mid \begin{smallmatrix} 18 \\ 5 \end{smallmatrix}) \xrightarrow{(R_1-3R_2)} (\begin{smallmatrix} 1 & -3 \\ 0 & -3 \end{smallmatrix} \mid \begin{smallmatrix} 18 \\ 5 \end{smallmatrix}) \xrightarrow{(R_2-R_1)} (\begin{smallmatrix} 1 & -3 \\ 0 & 0 \end{smallmatrix} \mid \begin{smallmatrix} 18 \\ 5 \end{smallmatrix})$ . So  $2 \times 18 - 7 \times 5 = 1$ ;  $(-7) \times 5 \equiv 1 \pmod{18}$ ;  $-7 \equiv 11 \pmod{18}$ . So  $5^{-1} = 11$  and  $11^{-1} = 5$ .  

<b>a</b>	1	5	7	11	13	17
<b>a<sup>-1</sup></b>	1	11	13	5	7	17

 Similarly for the *others*.

We can often use the **decomposition of 1** as a quick alternative. To solve  $5x \equiv 7 \pmod{18}$ , multiply by  $5^{-1} \equiv 11$  to get  $(11 \times 5)x \equiv 11 \times 7 \pmod{18}$ ;  $x \equiv 77 \equiv 5 \pmod{18}$ . [**Here**  $5 \times 5 \equiv 25 \equiv 7 \pmod{18}$ ]. **Example:** Find all *inverses* in  $\mathbf{Z}_{17}^*$ . 17 is *prime*, so  $U(\mathbf{Z}_{17}^*) = \mathbf{Z}_{17}^*$ . *Decomposing* (mod 17),  $1 \equiv 18 \equiv 2 \times 9 \equiv (-2) \times (-9) \equiv 15 \times 8$ . And  $1 \equiv 18 \equiv 3 \times 6 \equiv (-3) \times (-6) \equiv 14 \times 11$ . And  $1 \equiv 35 \equiv 7 \times 5 \equiv (-7) \times (-5) \equiv 10 \times 12$ .  
 And  $1 \equiv (-1) \times (-1) \equiv$   

<b>a</b>	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
<b>a<sup>-1</sup></b>	1	9	6	13	7	3	5	15	2	12	14	10	4	11	8	16

**16**×**16**. Finally,  $1 \equiv -16 \equiv 4 \times (-4) \equiv 4 \times 13$ .

8th February 2000

Q: Find the *multiplicative inverse* of 8 in  $\mathbf{Z}_{13}^*$  by the matrix method. Hence solve  $8x \equiv 10 \pmod{13}$ . A: **Find**  $\gcd(8,13) = 1 = -3 \times 13 + 5 \times 8$ . Hence  $8^{-1} \equiv 5$ . **Now** in  $8x \equiv 10 \pmod{13}$ , multiply by  $8^{-1} \equiv 5$  to give  $x \equiv 50 \pmod{13}$ ;  $x \equiv 11 \pmod{13}$ . Q: Find all **inverses** in  $\mathbf{Z}_{19}^*$ . A: Use the *decomposition of 1* method, pairing things off, e.g.  $1 \equiv 20 \equiv 2 \times 10 \equiv 4 \times 5 \equiv (-4) \times (-5) \equiv 15 \times 14$ , etc.

## Euler's $\phi$ Function

**Definition:** For  $m \in \mathbf{Z}^+$ , we define  $\phi(m)$  as the *number of integers* between 1 &  $m$  (inclusive) relatively prime to  $m$ . Example: if  $m = 18$ , then 1, 5, 7, 11, 13 and 17 are *relatively prime* to 18, so that  $\phi(18) = 6$ . **Notes.** (i) if  $p$  is prime, then  $\phi(p) = (p-1)$ , because  $1, 2, \dots, (p-1)$  are relatively prime to  $p$ . (ii)  $\phi(m) =$  the number of *invertible elements* in  $\mathbf{Z}_m^* =$  the number of elements in  $U(\mathbf{Z}_m^*)$ .

(iii) if  $p$  is prime, then  $\phi(p^\alpha) = p^\alpha - p^{\alpha-1}$ . **Proof.** The *only* numbers between 1 and  $p^\alpha$  which are **not** relatively prime to  $p^\alpha$  are the *multiples* of  $p$ :  $1p, 2p, 3p, \dots, p^{(\alpha-1)}p = p^\alpha$ . There are a total of  $p^{\alpha-1}$  of these numbers. **All** of the other  $p^\alpha$  numbers **will** be *relatively prime*, so that  $\phi(p^\alpha) = p^\alpha - p^{\alpha-1}$ . Example:  $\phi(16) = \phi(2^4) = 2^4 - 2^3 = 8$ . (iv) If  $p_1$  &  $p_2$  are *distinct primes*, and  $m = p_1^{\alpha_1} p_2^{\alpha_2}$ , then  $\phi(m) = \phi(p_1^{\alpha_1} p_2^{\alpha_2}) = m(1 - 1/p_1)(1 - 1/p_2) = p_1^{\alpha_1} p_2^{\alpha_2} (1 - 1/p_1)(1 - 1/p_2) = (p_1^{\alpha_1} - p_1^{\alpha_1-1})(p_2^{\alpha_2} - p_2^{\alpha_2-1}) = \phi(p_1^{\alpha_1})\phi(p_2^{\alpha_2})$ .

**Proof.** We *count* the numbers between 1 &  $m$  which are not relatively prime to  $p_1^{\alpha_1} p_2^{\alpha_2}$ . The *multiples* of  $p_1$  are  $p_1, 2p_1, 3p_1, \dots, (m/p_1) \cdot p_1$ . The *multiples* of  $p_2$  are  $p_2, 2p_2, \dots, (m/p_2) \cdot p_2$ . There are  $m/p_1 + m/p_2$  of these. But *some* of these will be duplicated, **namely** the multiples of  $p_1 p_2$ :  $p_1 p_2, 2p_1 p_2, \dots, (m/p_1 p_2) p_1 p_2$ . There are  $(m/p_1 p_2)$  of these. Hence  $(m/p_1 + m/p_2 - m/p_1 p_2)$  numbers are **not** relatively prime to  $m$ . Therefore,  $\phi(m) = m - (m/p_1 + m/p_2 - m/p_1 p_2) = m(1 - 1/p_1 - 1/p_2 + 1/p_1 p_2) = m(1 - 1/p_1)(1 - 1/p_2)$ .

(iv) In general, if  $m = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_r^{\alpha_r}$  is the prime *factorisation* of  $m$  into powers of distinct primes, then  $\phi(m) = M(1 - 1/p_1) \dots (1 - 1/p_r) = \phi(p_1^{\alpha_1})\phi(p_2^{\alpha_2}) \dots \phi(p_r^{\alpha_r})$ . (Proof by **induction**). Examples:  $\phi(18) = \phi(2 \times 3^2) = \phi(2)\phi(3^2) = (2-1)(3^2-3) = 6$ ;  $\phi(135) = \phi(3^3 \times 5) = (3^3-3^2)(5-1) = 72$ ;  $\phi(30) = \phi(2 \times 3 \times 5) = (2-1)(3-1)(5-1) = 8$ ; and  $\phi(97) = 96$ .

9th February 2000

## Modular Matrix Algebra

Using the *addition & multiplication* for  $\mathbf{Z}_m$ , it is possible to perform matrix algebra with matrices over  $\mathbf{Z}_m$ . However, it is necessary to be *careful* in the use of multiplication, since not all members of  $\mathbf{Z}_m$  are invertible. We confine ourselves to  $2 \times 2$  matrices over  $\mathbf{Z}_m$ . **Theorem:**  $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$  (with  $a, b, c, d \in \mathbf{Z}_m$ ) is invertible iff  $\det(A)$  is *invertible* in  $\mathbf{Z}_m$ . In this case,  $A^{-1} = (\det(A))^{-1} \begin{pmatrix} d & -b \\ -c & a \end{pmatrix}$ . **Proof.** If  $A$  is invertible, then *there exists* an  $A^{-1}$  s.t.  $AA^{-1} = A^{-1}A = I$ , and so  $\det(AA^{-1}) \equiv (\det(A))(\det(A^{-1})) \equiv \det(I) \equiv 1 \pmod{m}$ . If  $\det(A)$  is *invertible* in  $\mathbf{Z}_m$ , then  $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} d & -b \\ -c & a \end{pmatrix} = \begin{pmatrix} ad-bc & -ab+ab \\ cd-cd & -bc+ad \end{pmatrix} = \begin{pmatrix} \det(A) & 0 \\ 0 & \det(A) \end{pmatrix} = \det(A) \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ . **Example:**  $A = \begin{pmatrix} 3 & 1 \\ 1 & 2 \end{pmatrix}$  over  $\mathbf{Z}_{26}$ .  $\det(A) = 5$ , and since  $26 = 2 \times 13$ , 5 is relatively prime to 26 — and is *invertible*. By computing *multiples* of 26 (26, 52, 78, 104, ...), we see that  $5 \times 21 = 105 \equiv 1 \pmod{26}$ . So  $5^{-1} \equiv 21$ . Therefore,  $A^{-1} \equiv 21 \begin{pmatrix} 2 & -1 \\ -1 & 3 \end{pmatrix} = \begin{pmatrix} 42 & -21 \\ -21 & 63 \end{pmatrix} \equiv \begin{pmatrix} 16 & 5 \\ 5 & 11 \end{pmatrix} \pmod{26}$ .

## Hill 2-cyphers

*Suppose* that we have a message (in plain text) which we wish to encode. Assign to each **letter** a number in  $\mathbf{Z}_{26}$  (e.g.  $A = 1, B = 2, \dots, Z = 26$ ). Let  $A$  be a  $2 \times 2$  invertible matrix over  $\mathbf{Z}_{26}$ . Break the message into pairs of numbers, and multiply each 2 dimensional vector by  $A$ . This gives the **cyphertext**. To decode, simply multiply each *pair* by  $A^{-1}$  & reconvert to letters.

**Example:**  $A = \begin{pmatrix} 3 & 1 \\ 1 & 2 \end{pmatrix}$ ; plain text “Matrix”. Converting into numbers, we have 13, 1, 20, 18, 9 and 24, or the three vectors  $\begin{pmatrix} 13 \\ 1 \end{pmatrix}$ ,  $\begin{pmatrix} 20 \\ 18 \end{pmatrix}$  and  $\begin{pmatrix} 9 \\ 24 \end{pmatrix}$ . *Multiply by A:*  $\begin{pmatrix} 3 & 1 \\ 1 & 2 \end{pmatrix} \begin{pmatrix} 13 \\ 1 \end{pmatrix} \equiv \begin{pmatrix} 40 \\ 15 \end{pmatrix} \equiv \begin{pmatrix} 14 \\ 15 \end{pmatrix} \pmod{26}$ ;  $\begin{pmatrix} 3 & 1 \\ 1 & 2 \end{pmatrix} \begin{pmatrix} 20 \\ 18 \end{pmatrix} \equiv \begin{pmatrix} 78 \\ 56 \end{pmatrix} \equiv \begin{pmatrix} 0 \\ 4 \end{pmatrix} \pmod{26}$ ; and  $\begin{pmatrix} 3 & 1 \\ 1 & 2 \end{pmatrix} \begin{pmatrix} 9 \\ 24 \end{pmatrix} \equiv \begin{pmatrix} 51 \\ 57 \end{pmatrix} \equiv \begin{pmatrix} 25 \\ 5 \end{pmatrix} \pmod{26}$ . *The cyphertext is* 14, 15, 0, 4, 25 and 5, or “NOZDYE”. *Decoding,*  $A^{-1} = \begin{pmatrix} 16 & 5 \\ 5 & 11 \end{pmatrix}$ . So, for example,  $\begin{pmatrix} 16 & 5 \\ 5 & 11 \end{pmatrix} \begin{pmatrix} 14 \\ 15 \end{pmatrix} \equiv \begin{pmatrix} 299 \\ 235 \end{pmatrix} \equiv \begin{pmatrix} 13 \\ 1 \end{pmatrix} \pmod{26}$ , i.e. MA. **Example:**  $A = \begin{pmatrix} 1 & 0 \\ 4 & 3 \end{pmatrix}$ ; plain text “Maths”. Firstly, add an extra Z to the plain text to give an even number of letters. Secondly, find  $A^{-1} = (\det(A))^{-1} \begin{pmatrix} d & -b \\ -c & a \end{pmatrix}$ . We know that  $\det(A) = 3$ , so let us find  $3^{-1}$ :  $1 \equiv 27 \equiv 3 \times 9$ ; so  $3^{-1} \equiv 9$ . Therefore,  $A^{-1} = 9 \begin{pmatrix} 3 & -4 \\ -1 & 1 \end{pmatrix} = \begin{pmatrix} 27 & -36 \\ -9 & 9 \end{pmatrix} \equiv \begin{pmatrix} 1 & 0 \\ 16 & 9 \end{pmatrix}$ . Now MATHSZ becomes 13, 1, 20, 8, 19 and 26. So  $\begin{pmatrix} 1 & 0 \\ 4 & 3 \end{pmatrix} \begin{pmatrix} 13 \\ 1 \end{pmatrix} \equiv \begin{pmatrix} 13 \\ 55 \end{pmatrix} \equiv \begin{pmatrix} 13 \\ 3 \end{pmatrix}$ ;  $\begin{pmatrix} 1 & 0 \\ 4 & 3 \end{pmatrix} \begin{pmatrix} 20 \\ 8 \end{pmatrix} \equiv \begin{pmatrix} 20 \\ 104 \end{pmatrix} \equiv \begin{pmatrix} 20 \\ 26 \end{pmatrix}$ ; and  $\begin{pmatrix} 1 & 0 \\ 4 & 3 \end{pmatrix} \begin{pmatrix} 19 \\ 26 \end{pmatrix} \equiv \begin{pmatrix} 19 \\ 154 \end{pmatrix} \equiv \begin{pmatrix} 19 \\ 24 \end{pmatrix}$ . *The cyphertext is* 13, 3, 20, 26, 19 and 24, or MCTZSX. **Decoding,**  $\begin{pmatrix} 1 & 0 \\ 16 & 9 \end{pmatrix} \begin{pmatrix} 13 \\ 3 \end{pmatrix} \equiv \begin{pmatrix} 13 \\ 235 \end{pmatrix} \equiv \begin{pmatrix} 13 \\ 1 \end{pmatrix} = \text{MA}$ ;  $\begin{pmatrix} 1 & 0 \\ 16 & 9 \end{pmatrix} \begin{pmatrix} 20 \\ 26 \end{pmatrix} \equiv \begin{pmatrix} 20 \\ 554 \end{pmatrix} \equiv \begin{pmatrix} 20 \\ 8 \end{pmatrix} = \text{TH}$ ; and  $\begin{pmatrix} 1 & 0 \\ 16 & 9 \end{pmatrix} \begin{pmatrix} 19 \\ 24 \end{pmatrix} \equiv \begin{pmatrix} 19 \\ 520 \end{pmatrix} \equiv \begin{pmatrix} 19 \\ 26 \end{pmatrix} = \text{SZ}$ .

## Chapter 2: Binary Operations

**Definition:** If the number of elements in a set  $S$  is a *finite* number “ $n$ ”, then we say that  $S$  has “*order*  $n$ ”, and write  $|S| = n$ . **Definition:** If  $A$  and  $B$  are sets, then their “*product*”  $A \times B$  is defined to be the set of all **ordered** pairs of elements from  $A$  and  $B$ :  $A \times B = \{(x,y) : x \in A, y \in B\}$ .

### Relations

**Definition:** A relation “ $\sim$ ” on a set  $S$  is a set of *ordered pairs*  $(x,y)$ , with  $x, y \in S$ . If  $(x,y) \in \sim$ , we write  $x \sim y$ . (i) “ $\sim$ ” is **reflexive** iff  $x \sim x$  for all  $x \in S$ . (ii)  $\sim$  is **symmetric** iff  $x \sim y \Rightarrow y \sim x$  for all  $x, y \in S$ . (iii)  $\sim$  is **transitive** iff  $x \sim y$  and  $y \sim z \Rightarrow x \sim z$  for all  $x, y, z \in S$ . **Definition:** A relation which is *reflexive, symmetric & transitive* is called an equivalence relation.

**Example:** For a fixed positive integer  $m$ ,  $a \equiv b \pmod{m}$  is an *equivalence relation* on  $\mathbf{Z}$ . **Reflexive:**  $a \equiv a \pmod{m}$  for all  $a \in \mathbf{Z}$ , since  $(a-a)$  is *divisible* by  $m$ . **Symmetric:**  $a \equiv b \pmod{m} \Rightarrow b \equiv a \pmod{m}$ , since  $(a-b)$  is divisible by  $m \Rightarrow (b-a)$  is divisible by  $m$ . **Transitive:**  $a \equiv b \pmod{m} \Rightarrow (a-b) = km$ ;  $b \equiv c \pmod{m} \Rightarrow (b-c) = lm$ ; so  $a-c = (a-b) + (b-c) = km + lm = (k+l)m$ , i.e.  $(a-c)$  is *divisible* by  $m$ , so that  $a \equiv c \pmod{m}$ . **Example:** Define  $\sim$  on  $\mathbf{R}$  by  $x \sim y \Leftrightarrow xy \geq 0$ . **Reflexive:**  $xx \geq 0$  always **because**  $(+ve)(+ve) = +ve$  and  $(-ve)(-ve) = +ve$ . **Symmetric:** If  $xy \geq 0$ , then  $yx \geq 0$  follows from the *commutativity of multiplication*. **Transitive:** we need 1 **counter** example: Let  $x = 1$ ,  $y = 0$ , and  $z = -1$ . Then  $xy \geq 0$  and  $yz \geq 0$ , **but**  $xz \not\geq 0$ .

15th February 2000

**Definition:** If  $\sim$  is an *equivalence relation* on a set  $S$ , then we define the equivalence class of  $x$  by  $[x] = \{t \in S : t \sim x\}$ . **Notes:** (i)  $x \in [x]$ . ( $x \sim x$ ). (ii)  $[x] = [y] \Leftrightarrow x \sim y$ . If  $[x] = [y]$ , then  $y \in [x] \Rightarrow y \sim x$ . If  $x \sim y$ , then  $t \in [x] \Rightarrow t \sim x$ . But,  $x \sim y$ , and so by *transitivity*,  $t \sim y \Rightarrow t \in [y]$ , and hence  $[x] \subseteq [y]$ . Similarly,  $[y] \subseteq [x]$ . **Example:** For congruence *mod*  $m$  on  $\mathbf{Z}$ ,  $[x] = \{t \in \mathbf{Z} : x \equiv t \pmod{m}\}$ . We *usually* take  $x$  (the representative of the class) from the set  $\mathbf{Z}_m = \{0,1,\dots,(m-1)\}$ , e.g.  $m = 3$ :  $\mathbf{Z}_3 = \{0,1,2\}$ , where  $[0] = \{\dots,-3,0,3,6,\dots\}$ ;  $[1] = \{\dots,-2,1,4,7,\dots\}$ ; and  $[2] = \{\dots,-1,2,5,8,\dots\}$ . **Definition:** A *partition* of a set  $S$  is a set of non-empty subsets of  $S$   $\{S_1, S_2, \dots, S_k\}$  such that (i)  $S = S_1 \cup S_2 \cup \dots \cup S_k$ ; (ii)  $S_i \cap S_j = \emptyset$  if  $i \neq j$  (*disjoint*).

**Theorem:** If  $\sim$  is an *equivalence relation* on  $S$ , then the equivalence classes form a partition of  $S$ . Conversely, any **partition** of  $S$  defines an *equivalence relation* on  $S$ . **Proof:** Let  $\sim$  be an *equivalence relation* on  $S$ . Since  $x \in [x]$  for all  $x \in S$ , then the *union* of all equivalence classes **is**  $S$ . ((i) satisfied).

Now suppose that for 2 different equivalence classes  $[x]$  and  $[y]$ , we have  $t \in [x]$  and  $t \in [y]$ . Then  $x \sim t$  and  $t \sim y$ , and by **transitivity**, this gives  $x \sim y \Rightarrow [x] = [y]$ , i.e. a contradiction to our assumption that **different** classes can have **common** elements. ((ii) satisfied). Let  $\{S_1, S_2, \dots, S_k\}$  be a *partition* of  $S$ . Define  $\sim$  by  $x \sim y \Leftrightarrow x$  and  $y$  are in the **same** subset of the partition. This is **reflexive**, **symmetric** and **transitive**.

Q: Let  $x = \{1,2,3,4,5,6\}$ , and let  $P$  be the *partition* of  $X$  given by  $P = \{\{1,2\}, \{3\}, \{4,5,6\}\}$ . List all the *ordered* pairs in the equivalence relation defined on  $X$  by  $P$ . This is given by  $1 \sim 1, 1 \sim 2, 2 \sim 1, 2 \sim 2, 3 \sim 3, 4 \sim 4, 4 \sim 5, 5 \sim 4, 4 \sim 6, 6 \sim 4, 5 \sim 6, 6 \sim 5, 5 \sim 5$  and  $6 \sim 6$ .

**Example:** for  $\equiv \pmod{m}$  on  $\mathbf{Z}$ , the *equivalence classes*  $[0], [1], \dots, [m-1]$  which *partition*  $\mathbf{Z}$  are called "residue classes". We define **addition** & **multiplication** of *residue* classes as follows:  $[a]+[b] = [a+b]$ ;  $[a]\times[b] = [a\times b]$ . Example: for  $m = 3$ , we have  $[2]\times[2] = \{\dots, -1, 2, 5, \dots\} \times \{\dots, -1, 2, 5, \dots\} = [2\times 2] = [4] = [1] = \{\dots, -2, 1, 4, 7, \dots\}$ .

**Consistency.** We must show that these *definitions* are independent of the particular  $a$  and  $b$  we choose to represent the residue class (e.g.  $[5]\times[-1] = [1]$ ?). **Suppose** that we choose  $x$  as representative of the class  $[a]$ ; (i.e.  $[x] = [a]$ ); and choose  $y$  as representative of the class  $[b]$ . (i.e.  $[y] = [b]$ ). *Does it follow that*  $[x+y] = [a+b]$  and  $[x\times y] = [a\times b]$ ?

**Now**  $a \equiv x \pmod{m}$  and  $b \equiv y \pmod{m} \Rightarrow a = x+km$  and  $b = y+lm$ , for some  $k, l \in \mathbf{Z}$ . So  $a+b = (x+y)+(k+l)m \Rightarrow a+b \equiv x+y \pmod{m} \Rightarrow [x+y] = [a+b]$ . Similarly,  $a\times b = (x+km)(y+lm) = xy+(lx+ky+klm)m \Rightarrow a\times b \equiv xy \pmod{m}$ ;  $[a\times b] = [x\times y]$ . When we do *modular arithmetic*, we are just **adding** & **multiplying** the residue classes, but *omitting* the  $[ \ ]$ .

## Assignment 1: Set 15/2; In 22/2; Back 23/2

Q: Use the **matrix** method to find the *multiplicative inverse* of 338 in  $\mathbf{Z}_{387}^*$ , and hence *solve*  $338x \equiv 385 \pmod{387}$ . A: Using the *matrix* method, we find that  $\gcd(338, 387) = 1 = 69\times 387 - 79\times 338$ . So  $338^{-1} \equiv -79 \equiv -79+387 \equiv 308 \pmod{387}$ . In  $338x \equiv 385 \pmod{387}$ , multiplying *through* by  $338^{-1} \equiv 308$  gives  $x \equiv 118580 \pmod{387}$ ;  $x \equiv 158 \pmod{387}$ . (Because  $385\times 308 = 118580 = 306\times 387 + 158$ ).

Q: Find all **inverses** in  $\mathbf{Z}_{29}^*$ . (29 is *prime*, so  $U(\mathbf{Z}_{29}^*) = \mathbf{Z}_{29}^*$ ). A: Decomposing 1 *mod* 29, we get e.g.  $1 \equiv 30 \equiv 2\times 15 \equiv (-2)\times(-15) \equiv 27\times 14$ , and so on, filling in a *table*. Remember that when doing this, you can go in the *negative* direction as well — e.g.  $1 \equiv -28 \equiv 4\times(-7) \equiv 4\times 22$ . Finally, remember that the *first* and *last* elements are always inverses of **themselves**, as  $1 \equiv 1\times 1 \equiv (-1)\times(-1) \equiv 28\times 28$ .

Q: **Find**  $\phi(4346)$ . A:  $\phi(4346) = \phi(2 \times 41 \times 53) = \phi(2)\phi(41)\phi(53) = (2-1)(41-1)(53-1) = 2080$ .

Q: Find the *largest* value of  $\phi(m)$  for  $m < 1000$ . A: The *definition* says that  $\phi(m)$  is the number of integers between 1 and  $m$  (inclusive) *relatively prime* to  $m$ .

Common sense says to look for the **largest** prime number less than 1000, because if  $p$  is prime, and  $p > a$ , then  $\phi(p) > \phi(a)$  for all  $p$  and  $a$ . Now 997 is the prime *closest* to 1000, and so  $\phi(997) = 996 > \phi(n)$  for  $n = 1, \dots, 996$ . As  $998 = 499 \times 2$ , and  $999 = 333 \times 3$ , then the *largest* value of  $\phi(m)$  for  $m < 1000$  is 996, which comes from  $\phi(997)$ .

Q: **Using** a Hill-2 cipher with *enciphering* matrix  $A = \begin{bmatrix} 1 & 2 \\ 0 & 3 \end{bmatrix}$  over  $\mathbf{Z}_{26}$ , *encipher* the message "I AM IN HIDING". Find the **inverse** of  $A$  over  $\mathbf{Z}_{26}$ , and use it to check by *deciphering the first* 2 letters. A: Add a  $Z$  to the end, so that we have an *even* number of letters. The message IAMINHIDINGZ becomes 9, 1, 13, 9, 14, 8, 9, 4, 9, 14, 7 and 26; or  $\binom{9}{1}$ ,  $\binom{13}{9}$ , ...

*Encoding*, we do e.g.  $\binom{1}{0} \binom{2}{3} \binom{9}{1} \equiv \binom{11}{3} \pmod{26}$ ;  $\binom{1}{0} \binom{2}{3} \binom{13}{9} \equiv \binom{31}{27} \equiv \binom{5}{1} \pmod{26}$ ; ... To *decipher*, calculate  $A^{-1}$  and do  $(A^{-1})(\text{new vectors})$ . Remember that  $A^{-1} = (\det(A))^{-1} \begin{pmatrix} d & -b \\ -c & a \end{pmatrix}$ , and that we must calculate the inverse of the determinant *modularly* i.e.  $3^{-1} \equiv 9 \pmod{26}$ .

16th February 2000

## Functions

A *function*  $f$  from a set  $\mathbf{A}$  to a set  $\mathbf{B}$ ,  $f: \mathbf{A} \rightarrow \mathbf{B}$ , associates for *every*  $x \in \mathbf{A}$  a unique  $y \in \mathbf{B}$ , such that  $y = f(x)$ .  $\mathbf{A}$  is the **domain** of  $f$ , and  $\mathbf{B}$  is the **codomain** of  $f$ . The **image** of  $f$  is the *set of images*  $f(\mathbf{A}) = \{y \in \mathbf{B} : f(x) = y \text{ for some } x \in \mathbf{A}\}$ .  $f$  is *injective* (one-to-one) iff  $f(x_1) = f(x_2) \Rightarrow x_1 = x_2$ .  $f$  is *surjective* (onto) iff  $f(\mathbf{A}) = \mathbf{B}$ .  $f$  is *bijective* iff  $f$  is *surjective* and *injective*.

**Let**  $f: \mathbf{A} \rightarrow \mathbf{B}$  and  $g: \mathbf{B} \rightarrow \mathbf{C}$  be functions. The **composite** function,  $g \circ f: \mathbf{A} \rightarrow \mathbf{C}$ , is *defined* by  $(g \circ f)(x) = g(f(x))$  for all  $x \in \mathbf{A}$ . We **denote** by  $\mathbf{B}^{\mathbf{A}}$  the set of *all functions*  $f: \mathbf{A} \rightarrow \mathbf{B}$ . **Example:**  $\mathbf{A} = \{a, b\}$ ;  $\mathbf{B} = \{1, 2\}$ . Here,  $\mathbf{B}^{\mathbf{A}}$  is  $\{a \rightarrow 1, b \rightarrow 1; \{a \rightarrow 1, b \rightarrow 2; \{a \rightarrow 2, b \rightarrow 1; \{1 \rightarrow 2, b \rightarrow 2$ . For the first one,  $f(\mathbf{A}) = \{1\}$ ; the *second* and *third* are **bijective**, and for the *fourth*,  $f(\mathbf{A}) = \{2\}$ . **Note that**  $|\mathbf{B}^{\mathbf{A}}| = 4 = 2^2 = |\mathbf{B}|^{|\mathbf{A}|}$ . This is true in *general*.

**Example:** Let  $f: \mathbf{X} \rightarrow \mathbf{Y}$  be a *function*. Define a relation  $\sim$  **on**  $\mathbf{X}$  by  $x_1 \sim x_2 \Leftrightarrow f(x_1) = f(x_2)$ . Now prove that it is an *equivalence* relation. (1): **Reflexive:**  $x \sim x$  since  $f(x) = f(x)$  for *all*  $x \in \mathbf{X}$ . (2): **Symmetric:**  $x_1 \sim x_2 \Rightarrow f(x_1) = f(x_2) \Rightarrow f(x_2) = f(x_1) \Rightarrow x_2 \sim x_1$ . (3): **Transitive:**  $x_1 \sim x_2$  and  $x_2 \sim x_3 \Rightarrow f(x_1) = f(x_2)$  and  $f(x_2) = f(x_3)$ , which *imply that*  $f(x_1) = f(x_3) \Rightarrow x_1 \sim x_3$ .

**Example:** Define  $f: \mathbf{N} \rightarrow \mathbf{Z}$  by  $f(n) = n/2$  if  $n$  is *even*, and  $f(n) = -(n+1)/2$  if  $n$  is *odd*. We show that  $f$  is a *bijection*. First, note that  $f(n) \geq 0 \Rightarrow f(n) = n/2$  with  $n$  being *even*; and  $f(n) < 0 \Rightarrow f(n) = -(n+1)/2$  with  $n$  being *odd*. **Injective:** Suppose that  $f(p) = f(q) \geq 0$ , then  $f(p) = p/2 = f(q) = q/2 \Rightarrow p = q$ . *Similarly*,  $f(p) = f(q) < 0$  gives  $f(p) = -(p+1)/2 = -(q+1)/2 = f(q) \Rightarrow p = q$ . **Surjective:** Let  $p \in \mathbf{Z}$ . If  $p \geq 0$ , then  $2p$  is even, and  $f(2p) = p$ . If  $p < 0 \Rightarrow -2p-1$  is a *+ve odd number*, then  $f(-2p-1) = -((-2p-1)+1)/2 = p$ .

## The Pigeon-Hole Principle

Let  $X$  &  $Y$  be *finite* sets, and let  $f: X \rightarrow Y$  be a function. (i)  $f$  is **injective**  $\Leftrightarrow |f(x)| = |X|$ . (ii)  $f$  is **surjective**  $\Leftrightarrow |f(x)| = |Y|$ . (iii) If  $|X| = |Y|$ , then  $f$  is *injective* iff  $f$  is *surjective*. **Proof:** (i) Assume that  $|f(x)| = |X|$ , and let  $f(x_1) = f(x_2)$  for some  $x_1, x_2 \in X$ . If  $x_1 \neq x_2$ , then  $|f(x)| < |X|$ , since the *images* of two different elements in  $X$  would be the **same**. Therefore,  $f$  is **injective**. Now assume that  $f$  is injective, then the elements of  $f(x)$  are all *different*, and  $|f(x)| = |X|$ . (ii) Assume that  $|f(x)| = |Y|$ . Since  $f(x) \subseteq Y$ , then this can only mean that  $f(x) = Y$ . Assuming that  $f$  is *surjective*, then  $f(x) = Y$ , and  $|f(x)| = |Y|$ . (iii) **Combine** both the above!

## Binary Operations

**Definition:** A *binary operation*  $*$  on a set  $S$  is a function such that associated with each *ordered pair*  $(a,b)$  of elements of  $S$  is a uniquely defined element  $(a*b) \in S$ , i.e.  $*$ :  $S \times S \rightarrow S$ . **Examples:**  $+$  and  $\times$  are binary operations on  $\mathbf{Z}, \mathbf{R}, \mathbf{Q}, \mathbf{N}, \mathbf{C}, \mathbf{Z}_m$ ; and *matrices* over any of these. For any *set*  $S$ , we could have  $S^S$  with the **composition** of functions. A *binary operation* must be well defined (*for all*  $a, b \in S$ ).

**Example:** division is not a binary operation on  $\mathbf{R}$ , since  $a*b: a/b$  is not defined for  $b = 0$ . A binary operation must be *closed*:  $(a*b) \in S$  for all  $a, b \in S$ . Example: *division* is not a binary operation on  $\mathbf{Z}$  since  $(a*b) = a/b \notin \mathbf{Z}$  for  $b \neq 1$ . We can often get around such *problems* by changing the set  $S$ . For example, division is *well defined and closed* on  $S = (0, \infty)$ .

**Definition:** A *binary operation*  $*$  on a set  $S$  is **associative** iff  $(x*y)*z = x*(y*z)$  for all  $x, y, z \in S$ . **Examples:**  $+$  and  $\times$  are *associative* on  $\mathbf{Z}, \mathbf{R}, \mathbf{Q}, \mathbf{N}, \mathbf{C}, \mathbf{Z}_m$ ; *matrices* over these; and  $S^S$  with *function* composition. **However**, “ $-$ ” is a binary operation on  $\mathbf{Z}$  which is *well defined and closed*, but **not** associative:  $1-(2-3) \neq (1-2)-3$ . With *division* on  $S = (0, \infty)$ , we have  $(3/4)/5 \neq 3/(4/5)$ .

## General Associative Law

If  $*$  is *associative*, then it can be **proved** that  $a_1*a_2*...*a_n$  has a *unique* value which is **independent** of the brackets. **Definition:** If  $*$  is a *binary operation* on  $S$ , then if  $e \in S$  is s.t.  $x*e = e*x = x$  for all  $x \in S$ , then we **call**  $e$  the “*identity element*”. **Note:** If  $e$  exists, then it is *unique*, for suppose that  $e_1$  and  $e_2$  are **both** identity elements, then  $e_1 = e_1*e_2 = e_2$  by their *definition*.

**Examples:**  $+$  on  $\mathbf{Z}, \mathbf{R}, \mathbf{Q}, \mathbf{C}$  and  $\mathbf{Z}_m$  has  $0$  as the *identity element*;  $\times$  on the same save  $\mathbf{Z}_m$  has  $1$  as the *identity element*. For **matrices**,  $+$  has the *zero matrix* as identity;  $\times$  has the *identity matrix*  $I$  as identity. For  $S^S$  with *composition of functions*, the **identity** element is the identity function  $I_s$  defined by  $I_s(x) = x$  for all  $x \in S$ .

**Definition:** Let  $S$  be a set with a *binary operation*  $*$  and an identity element  $e$ . If for **some**  $x \in S$  we have  $x*(x^{-1}) = (x^{-1})*x = e$ , with  $x^{-1} \in S$ , we say that  $(x^{-1})$  is an inverse for  $x$ . **Notes:** (i) If  $*$  is *associative*, then any inverse of  $x$  will be **unique**; and (ii) if  $x$  and  $y$  *both* have inverses, and  $*$  is *associative*, then the **inverse** of  $x*y$  is  $y^{-1}*x^{-1} = (x*y)^{-1}$ .

**Examples:** + on  $\mathbf{Z}, \mathbf{R}, \mathbf{Q}, \mathbf{C}, \mathbf{Z}_m$ ; ( $x$  has *inverse*  $x^{-1} = -x$ , where  $x^{-1} = (m-x)$  in  $\mathbf{Z}_m$ , etc.);  $\times$  on  $\mathbf{R}, \mathbf{Q}, \mathbf{C}$  ( $x$  has inverse  $1/x$ ). For  $\mathbf{Z}_m^*$ ,  $x$  has an inverse *iff*  $\gcd(x,m) = 1$ . For matrices, we require  $\det(A)$  to be invertible for the multiplicative inverse to exist.

22nd February 2000

## An Example

Let  $S = \mathbf{R} \setminus \{-1\}$ , and let  $*$  be *defined* by  $a*b = |^{a+1}_a^{-1}b| = ab+b+a = ab+a+b$ . This is *well defined* for all  $a,b \in S$ . Closure. Suppose that  $a*b = -1 = ab+a+b$ , i.e.  $a*b \notin S$  for some  $a,b \in S$ . This implies that  $ab+a+b+1 = 0 \Rightarrow (a+1)(b+1) = 0 \Rightarrow a = -1$  or  $b = -1$ . This is all right, and we conclude that  $a*b \in S$  for all  $a, b \in S$ . Associative.  $a*(b*c) = a*(bc+b+c) = a(bc+b+c)+a+bc+b+c = abc+ab+ac+bc+a+b+c$ . *Similarly*,  $(a*b)*c$  gives the **same** thing.

Identity. We require  $a*e = e*a = a$  for all  $a \in S$ . **So**  $ae+a+e = a$ ;  $ae+e = 0$ ;  $e(a+1) = 0$ . As  $a+1$  is *never zero*, we must have  $e = 0 \in S$ . **Check:**  $a*0 = a \times 0 + a + 0 = a$ . Inverses. We require  $a*a^{-1} = a^{-1}*a = e = 0$ . So  $aa^{-1}+a+a^{-1} = 0$ ;  $a^{-1}(a+1) = -a$ ;  $a^{-1} = -a/a+1$ . **Note:** This is *well defined* since  $a \neq -1$ . *Also*,  $-a/a+1 = -1 \Rightarrow a = a+1$ . (*Wrong*). So we will **always** have  $-a/a+1 \in S$ . **Check:**  $a*(-a/a+1) = -a^2/a+1+a-a/a+1 = -a^2/a+1+a-a/a+1 = -a^2+a^2+a-a/a+1 = 0$ .

Definitions. Let  $\{S, *\}$  be a set  $S$  with a *well defined and closed* binary operation  $*$ . (1) If  $*$  is associative, then  $\{S, *\}$  is a **semi-group**. (2) If  $*$  is associative and has an identity element  $e$ , then  $\{S, *\}$  is a **monoid**. (3) If  $*$  is associative, has an identity element  $e$ , and every element  $x \in S$  has an inverse  $x^{-1} \in S$ , then  $\{S, *\}$  is called a **group**. (4) If  $x*y = y*x$  for all  $x, y \in S$ , then  $*$  is commutative. (5) If  $\{S, *\}$  is a **group** and  $*$  is commutative, then  $\{S, *\}$  is a **commutative group** or an **Abelian group**.

Important Examples. (1) For a set  $S$ , the set of *all* functions  $f: S \rightarrow S$ , or  $S^S$  with the composition “o”, is a **monoid** called the full transformation monoid.  $f \in S^S$  is invertible *iff*  $f$  is bijjective. The invertible (*bijjective*) functions in  $S^S$  form a group (the *group of permutations of*  $S$ ). If  $S = \{a,b,\dots\}$  is **finite**, we can describe  $f: S \rightarrow S$  by a *double row*:  $(^a_{f(a)}, ^b_{f(b)}, ^c_{f(c)}, \dots)$ . In this case, the *invertible* functions form the symmetric group. (2) For  $\mathbf{Z}_m^* = \{1,2,\dots,(m-1)\}$  with *multiplication mod m*, the set of **invertible** elements  $U(\mathbf{Z}_m^*)$  form a group of size  $\phi(m)$ . If  $m$  is **prime**, then  $U(\mathbf{Z}_m^*) = \mathbf{Z}_m^*$  forms a group of *size*  $(m-1)$ .

23rd February 2000

## Chapter 3: Groups

### Multiplicative Groups

If  $G$  is a group with binary operation  $*$ , we will *write*  $*$  as multiplication, i.e.  $a*b$  is written as  $ab$ . The **identity**  $e$  will be written as  $1$ , and **inverses** will be written as  $x^{-1}$ . **Note:** If  $ab = c$ , then  $c^2 = c.c = (ab)(ab) = a(ba)b$ , NOT  $a^2b^2$ , since we cannot *assume that*  $ab = ba$ .

Powers of an element. If  $G$  is a group, and  $a \in G$ , *define*  $a^0 = 1$ ;  $a^1 = a$ ;  $a^2 = a.a$ ; etc., with  $a^{-1}$  = the *inverse* of  $a$ ; and  $a^{-n} = (a^{-1})^n$ . Then the *usual* rules apply:  $a^m.a^n = a^{m+n}$ ;  $(a^m)^n = a^{mn}$ . (For all  $m, n \in \mathbf{Z}$ ).

**Definitions:** (1) The *order* of a group  $G$  is  $|G|$ . (2) The *order* of an element  $x \in G$  is the smallest **positive** integer  $n$  such that  $x^n = 1$ . (Note: this may *not* exist). **Example:** Consider  $\mathbf{Z}_5^* = \{1,2,3,4\}$ , with *multiplication mod 5*. Since 5 is prime, this is a group of order 4.

Looking at the *table* on the right, we see that  $1^1 = 1$ , so 1 is of *order 1*.  $2^2 = 4$ ;  $2^3 = 8 = 3$ ;  $2^4 = 2 \times 3 = 1$ ; so 2 is of *order 4*.  $3^2 = 4$ ;  $3^3 = 3 \times 4 = 2$ .  $3^4 = 2 \times 2 = 1$ ; so 3 is of *order 4*. And  $4^2 = 1$ , so 4 is of *order 2*.

+	1	2	3	4
1	1	2	3	4
2	2	4	1	3
3	3	1	4	2
4	4	3	2	1

**Theorem:** For a *finite* group  $G$ , each row/column of the Cayley table contains every element of  $G$  exactly *once*. **Proof:** Fix on the row having first element  $a \in G$ . Define  $f_a: G \rightarrow G$  by  $f(x) = ax$  for all  $x \in G$ , i.e. the elements in our *row* are the  $f_a(G)$ . For **any**  $b \in G$ , put  $x = a^{-1}b$ , and then  $f_a(x) = a(a^{-1}b) = b$ . Thus  $f_a$  is *surjective*, and by the P.H.P.,  $f_a$  is also *injective*. The results for **columns** follows *similarly*.

**Q:** Find the **order** of each element of the *multiplicative group*  $\mathbf{Z}_7^*$ .  $1^1 = 1$ , so 1 is of *order 1*.  $2^2 = 4$ ;  $2^3 = 2 \times 4 = 8 = 1$ ; so 2 is of *order 3*.  $3^2 = 9 = 2$ ;  $3^3 = 2 \times 3 = 6$ ;  $3^4 = 3 \times 6 = 18 = 4$ ;  $3^5 = 4 \times 3 = 12 = 5$ ;  $3^6 = 5 \times 3 = 15 = 1$ ; so 3 is of *order 6*. And so on for 4, 5 and 6.

## Groups of Permutations

**Definition:** Let  $X$  be any set, then a *bijective* function  $f: X \rightarrow X$  is called a *permutation* of  $X$ . If  $X$  is a **finite** set  $X = \{1,2,\dots,n\}$ , then the group of *all permutations* of  $X$  is called the **symmetric group of degree  $n$** ,  $S_n$ . (The order of  $S_n$  is  $n!$ ). **Example:**  $X = \{1,2,3\}$ ;  $S_3$ . Using the notation of *chapter 2*, we have the following permutations:

$(\begin{smallmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{smallmatrix})$ ,  $(\begin{smallmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{smallmatrix})$ ,  $(\begin{smallmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{smallmatrix})$ ,  $(\begin{smallmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{smallmatrix})$ ,  $(\begin{smallmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{smallmatrix})$  and  $(\begin{smallmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{smallmatrix})$ . The first is the *Identity*  $I_x$ ; the 2<sup>nd</sup> and 3<sup>rd</sup> are obtained by **cycling** 1, 2 and 3; the 4<sup>th</sup> is when 1 is *fixed*; the 5<sup>th</sup> is when 2 is *fixed*; and the 6<sup>th</sup> is when 3 is *fixed*. Recall that the **binary operation** is function composition. Thus  $(\begin{smallmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{smallmatrix}) \bullet (\begin{smallmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{smallmatrix})$  is given by *applying*  $(\begin{smallmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{smallmatrix})$  first.

So  $1 \rightarrow 1 \rightarrow 2$ ;  $2 \rightarrow 3 \rightarrow 1$ ; and  $3 \rightarrow 2 \rightarrow 3$ , i.e.  $(\begin{smallmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{smallmatrix}) \bullet (\begin{smallmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{smallmatrix}) = (\begin{smallmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{smallmatrix}) = I$ . Similarly  $(\begin{smallmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{smallmatrix}) \bullet (\begin{smallmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{smallmatrix}) = (\begin{smallmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{smallmatrix}) = I$ . The *diagram* on the right shows a table with **all** the different compositions. Now, for *example*,  $(\begin{smallmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{smallmatrix})^3 = (\begin{smallmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{smallmatrix}) = I$ , so  $(\begin{smallmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{smallmatrix})$  is of *order 3*. Also notice that this group is **not** commutative  $(\begin{smallmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{smallmatrix}) \bullet (\begin{smallmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{smallmatrix}) = (\begin{smallmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{smallmatrix}) \neq (\begin{smallmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{smallmatrix}) = (\begin{smallmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{smallmatrix}) \bullet (\begin{smallmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{smallmatrix})$ .

	$(\begin{smallmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{smallmatrix})$	$(\begin{smallmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{smallmatrix})$	$(\begin{smallmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{smallmatrix})$	$(\begin{smallmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{smallmatrix})$	$(\begin{smallmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{smallmatrix})$	$(\begin{smallmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{smallmatrix})$
$(\begin{smallmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{smallmatrix})$	$(\begin{smallmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{smallmatrix})$	$(\begin{smallmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{smallmatrix})$	$(\begin{smallmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{smallmatrix})$	$(\begin{smallmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{smallmatrix})$	$(\begin{smallmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{smallmatrix})$	$(\begin{smallmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{smallmatrix})$
$(\begin{smallmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{smallmatrix})$	$(\begin{smallmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{smallmatrix})$	$(\begin{smallmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{smallmatrix})$	$(\begin{smallmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{smallmatrix})$	$(\begin{smallmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{smallmatrix})$	$(\begin{smallmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{smallmatrix})$	$(\begin{smallmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{smallmatrix})$
$(\begin{smallmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{smallmatrix})$	$(\begin{smallmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{smallmatrix})$	$(\begin{smallmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{smallmatrix})$	$(\begin{smallmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{smallmatrix})$	$(\begin{smallmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{smallmatrix})$	$(\begin{smallmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{smallmatrix})$	$(\begin{smallmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{smallmatrix})$
$(\begin{smallmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{smallmatrix})$	$(\begin{smallmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{smallmatrix})$	$(\begin{smallmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{smallmatrix})$	$(\begin{smallmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{smallmatrix})$	$(\begin{smallmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{smallmatrix})$	$(\begin{smallmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{smallmatrix})$	$(\begin{smallmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{smallmatrix})$
$(\begin{smallmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{smallmatrix})$	$(\begin{smallmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{smallmatrix})$	$(\begin{smallmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{smallmatrix})$	$(\begin{smallmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{smallmatrix})$	$(\begin{smallmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{smallmatrix})$	$(\begin{smallmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{smallmatrix})$	$(\begin{smallmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{smallmatrix})$
$(\begin{smallmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{smallmatrix})$	$(\begin{smallmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{smallmatrix})$	$(\begin{smallmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{smallmatrix})$	$(\begin{smallmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{smallmatrix})$	$(\begin{smallmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{smallmatrix})$	$(\begin{smallmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{smallmatrix})$	$(\begin{smallmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{smallmatrix})$

## Subgroups

**Definition:** Let  $G$  be a group. Then  $H \subseteq G$  is a subgroup of  $G$  if  $H$  is itself a **group** with the same *operation* as  $G$ . Alternative definitions follow on the next page....

**Alternative Definitions:** (a): (i)  $H \subseteq G$ ; (ii) If  $a, b \in H \Rightarrow ab \in H$ ; (iii) If  $a \in H \Rightarrow a^{-1} \in H$ . Therefore,  $H$  is *closed* w.r.t. products and inverses. The **other** group properties will follow for  $H$ . In particular, if  $a \in H$ , then  $a^{-1} \in H$  and  $aa^{-1} = 1 \in H$ , giving the *same identity* for  $H$  and  $G$ . (b): (i)  $H \subseteq G$ ; (ii) If  $a, b \in H \Rightarrow ab^{-1} \in H$ . (**Notes:**  $b \in H \Rightarrow bb^{-1} = 1 \in H$ ;  $1, b \in H \Rightarrow 1.b^{-1} = b^{-1} \in H$ ;  $a, b \in H \Rightarrow a.b^{-1} \in H \Rightarrow a(b^{-1})^{-1} = ab \in H$ ).

**Examples:** (1) In  $\mathbf{Z}_5^* = \{1,2,3,4\}$ ,  $H = \{1,4\}$  forms a *subgroup*, since “ $4^2 = 1$ ”. (2) The identity  $\{1\}$  **always** forms a subgroup. (3) In  $S_3$ , the set  $\{I, ({}^1_2 {}^2_3 {}^3_1), ({}^1_3 {}^2_1 {}^3_2)\}$  forms a *subgroup* (see the **Cayley** table).

## Cyclic Groups

A *cyclic group* is one in which **every** element can be written as a *power* of one element “ $a$ ” called a **generator**, i.e.  $G = \{x: x = a^r, r \in \mathbf{Z}\}$ . (Including *negative* powers). **Notes:** (1) The generator is *not* in general *unique*, e.g.  $\mathbf{Z}_5^* = \{1,2,3,4\}$  is *generated* by 2 (see earlier) or by 3. Note that in **both** cases,  $2^4 \equiv 3^4 \equiv 1$ , where 4 is the *order* of the group. If we look at the elements generated by 4, we obtain the **subgroup**  $\{1,4\}$ .

29th February 2000

(2) For any group  $G$ , the *powers* of any element “ $a$ ” form a **subgroup** (*cyclic*) of  $G$ ,  $H = \{x: x = a^r, r \in \mathbf{Z}\}$ , since (i)  $H \subseteq G$ , (ii) If  $x = a^r, y = a^s \in H$ , then  $xy^{-1} = a^r(a^s)^{-1} = a^r a^{-s} = a^{r-s} \in H$ . Example: in  $S_3$ , the powers of  $({}^1_2 {}^2_3 {}^3_1)$  generates the *subgroup*  $\{I, ({}^1_2 {}^2_3 {}^3_1), ({}^1_3 {}^2_1 {}^3_2)\}$ . (3) Any *cyclic group*  $G$  ( $G = \{x: x = a^r, r \in \mathbf{Z}\}$ ) is **Abelian** since  $a^r.a^s = a^{r+s} = a^{s+r} = a^s.a^r$ .

(4) If  $n$  is the *smallest positive integer* s.t.  $a^n = 1$  (i.e.  $n$  is the **order** of  $a$ ), then  $G = C_n = \{1, a, a^2, \dots, a^{n-1}\}$  is of finite order  $n$ . (There are precisely  $n$  *distinct elements* here, since if  $a^r = a^s, 0 \leq s < r < n$ , then  $a^{r-s} = 1$ , with  $0 < (r-s) < n$ ). If there is **no such**  $n$ , then  $G = C_\infty = \{\dots, a^2, a^{-1}, 1, a, a^2, \dots\}$  is an *infinite cyclic group*. For example,  $\mathbf{Z}$  with the binary operation of “*addition*” is generated by 1; has identity element 0; and is an **infinite** cyclic group.

(5) If  $x \in C_n = \{1, a, \dots, a^{n-1}\}$ , then  $x^n = 1$  for all  $x \in C_n$ , since  $x = a^r$  for some  $r < n$ ;  $x^n = (a^r)^n = (a^n)^r = 1^r = 1$ . **Example:** Consider  $C_6 = \{1, a, a^2, \dots, a^5\}$  (with  $a^6 = 1$ ), then  $a^5 = b$  is *also* a generator for  $C_6$ , since  $b^0 = 1$  (by definition);  $b = a^5$ ;  $b^2 = a^{10} = a^6.a^4 = a^4$ ;  $b^3 = a^{15} = a^3$ ;  $b^4 = a^{20} = a^2$ ; and  $b^5 = a^{25} = a$ . (Modular arithmetic on the *powers*). On the **other** hand,  $c = a^2$  just generates the *cyclic subgroup* of even powers of  $a$ . ( $c^0 = 1$ ;  $c = a^2$ ;  $c^2 = a^4$ ;  $c^3 = a^6 = 1$ , i.e.  $\{1, a^2, a^4\}$ ).

**Theorem:** The *cyclic group*  $C_n = \{1, a, a^2, \dots, a^{n-1}\}$  (with  $a^n = 1$ ) is generated by  $a^r$  iff  $\gcd(n, r) = 1$ . (**Relatively prime**). Proof: (i) If  $\gcd(n, r) = 1$ , *there exists*  $p$  and  $q$  s.t.  $pn + qr = 1$  and  $(a^r)^q = a^{rq} = a^{1-pn} = a^1(a^n)^{-p} = a^1.1 = a$ . Now  $(a^r)$  generates a *cyclic subgroup* of  $C_n$ , and since this subgroup **contains**  $a$  ( $= (a^r)^q$ ), it includes all powers of  $a$ .

(ii) If  $C_n$  is *generated* by  $a^r$ , then since  $a \in C_n$  for some  $q$ ,  $(a^r)^q = 1$ . Hence  $rq \equiv 1 \pmod{n}$ , i.e.  $rq = 1 + \lambda n$ , or  $rq + (-\lambda)n = 1$ . Hence  $\gcd(n, r) = 1$ . **Corollary:** The number of *distinct possible generators* of  $C_n$  is  $\phi(n)$ , since  $\phi(n)$  is the number of numbers **between** 1 and  $n$  which are relatively prime to  $n$ .

**Theorem:** If  $p$  is a prime number, then  $\mathbf{Z}_p^* = \{1, 2, \dots, (p-1)\}$  is a *cyclic group* of order  $(p-1)$  [under multiplication modulo  $p$ ]. **Examples:**  $\mathbf{Z}_7^* = \{1, 2, 3, 4, 5, 6\}$  is a cyclic of order 6 by the above. We search for a *generator*. Note: a generator must be of order 6, since we need  $a^6 = 1$ . 3 is a generator:  $3^2 \equiv 2 \pmod{7}$ ;  $3^3 \equiv 6 \pmod{7}$ ;  $3^4 \equiv 4 \pmod{7}$ ;  $3^5 \equiv 5 \pmod{7}$ ; and  $3^6 \equiv 1 \pmod{7}$ . The **other** generators are of the form  $3^r$ , where  $\gcd(b, r) = 1$ . The only *possibility* is  $r = 5$ , as  $3^5 \equiv 5$ . ( $\phi(6) = \phi(2 \times 3) = 2$ ).

1st March 2000

**Question:** Find a *generator* for  $\mathbf{Z}_{13}^* = \{1, \dots, 12\}$ , and hence find all **other** possible generators of  $\mathbf{Z}_{13}^*$ . A: We have a cyclic group of order 12. The generator must be of order 12, so we need  $a^{12} = 1$ . We notice that  $2^{12} \equiv 4096 \equiv 1 \pmod{13}$ . Now  $2^1 \equiv 2 \pmod{13}$ ;  $2^2 \equiv 4 \pmod{13}$ ;  $2^3 \equiv 8 \pmod{13}$ ;  $2^4 \equiv 3 \pmod{13}$ ;  $2^5 \equiv 6 \pmod{13}$ ;  $2^6 \equiv 12 \pmod{13}$ ;  $2^7 \equiv 11 \pmod{13}$ ;  $2^8 \equiv 9 \pmod{13}$ ;  $2^9 \equiv 5 \pmod{13}$ ;  $2^{10} \equiv 10 \pmod{13}$ ; and  $2^{11} \equiv 7 \pmod{13}$ .

We now need numbers *relatively prime* to 12. The other possible generators are of the form  $2^r$ , where  $r$  is relatively prime to 12, i.e.  $r = 1, 5, 7$  or  $11$ , giving **generators** 2, 6, 11 and 7 from the above calculations. Check:  $\phi(12) = \phi(2^2 \times 3) = (2^2 - 2)(3 - 1) = 4$ .

**Example:** Consider  $U(\mathbf{Z}_{12}^*)$ . But 12 is not prime, so  $U(\mathbf{Z}_{12}^*)$  consists of the invertible elements of  $\mathbf{Z}_{12}^*$ , which do form a group. The elements of  $U(\mathbf{Z}_{12}^*)$  will be the numbers in  $\mathbf{Z}_{12}^*$  relatively prime to 12.  $U(\mathbf{Z}_{12}^*) = \{1, 5, 7, 11\}$ , and it is a *group* under multiplication mod 12. Is this a cyclic group? Look for a generator:  $1^2 \equiv 1 \pmod{12}$ ;  $5^2 \equiv 25 \equiv 1 \pmod{12}$ ;  $7^2 \equiv 1 \pmod{12}$ ;  $11^2 \equiv 1 \pmod{12}$ , i.e. *all elements* are of order 1 or 2. There are no **generators**, so the group is not cyclic. In fact, 5, 7 and 11 each generate cyclic *subgroups* ( $\{1, 5\}$ ,  $\{1, 7\}$  and  $\{1, 11\}$ ).

Q: Show that  $U(\mathbf{Z}_9^*)$  is cyclic, and find all *possible* generators.  $U(\mathbf{Z}_9^*) = \{1, 2, 4, 5, 7, 8\}$ ;  $2^6 \equiv 64 \equiv 1 \pmod{9}$ . Now  $2^1 \equiv 2$ ;  $2^2 \equiv 4$ ;  $2^3 \equiv 8$ ;  $2^4 \equiv 7$ ;  $2^5 \equiv 5$ ; and  $2^6 \equiv 1$ . Thus we have a *cyclic group* of order 6 ( $\phi(6) = 2$ ). The only other **generator** is  $2^5 \equiv 5$ . ( $\gcd(5, 6) = 1$ ).

## Assignment 2: Set 29/2; In 7/3; Back 8/3

Q: Find functions  $\alpha: \mathbf{N} \rightarrow \mathbf{N}$  and  $\beta: \mathbf{N} \rightarrow \mathbf{N}$  such that  $\beta \circ \alpha$  is surjective, but  $\alpha$  is not surjective. A: There are many *solutions* possible, e.g. put  $\alpha(n) = n+1$  for all  $n \in \mathbf{N} = \{1, 2, 3, \dots\}$ ; then  $\alpha$  is *not surjective* since  $1 \notin \alpha(\mathbf{N})$ . Put  $\beta(n) = 1$  if  $n = 1$ ; and  $\beta(n) = n-1$  if  $n \geq 2$  (Note:  $\beta(n) \in \mathbf{N}$  for all  $n \in \mathbf{N}$ ). Then  $\beta \circ \alpha: \mathbf{N} \rightarrow \mathbf{N}$  has  $\beta \circ \alpha(1) = \beta(\alpha(1)) = \beta(2) = 2-1 = 1$ ; and for *all*  $n \geq 2$ ,  $\beta \circ \alpha(n) = \beta(\alpha(n)) = \beta(n+1) = n+1-1 = n$ . **Hence**  $(\beta \circ \alpha)(\mathbf{N}) = \mathbf{N}$ , and  $\beta \circ \alpha$  is *surjective*.

In general, to prove that  $\alpha$  is not a surjection, we need to find an element in the *co-domain* which is not the **image** of any element in the domain. To prove that  $\alpha$  is a surjection, we must find the element which maps onto any given element in the co-domain of  $\alpha$ .

Q: Consider the set of *all functions*  $f: S \rightarrow S$ , i.e.  $S^S$ , where  $S = \mathbf{R} \setminus \{0, 1\}$ . Let  $A = \{\alpha_1, \alpha_2, \alpha_3, \alpha_4, \alpha_5, \alpha_6\}$  be the subset of  $S^S$  given by  $\alpha_1(x) = x$ ;  $\alpha_2(x) = 1/x$ ;  $\alpha_3(x) = 1-x$ ;  $\alpha_4(x) = 1-1/x$ ;  $\alpha_5(x) = 1/(1-x)$ ; and  $\alpha_6(x) = x/(x-1)$ . (**All functions** for all  $x \in S$ ). By completing the Cayley Table, show that  $A$  is closed under the *binary operation of the composition of functions*.

A: *Complete* the table, and as (after manipulation) all elements of the table are also elements of A, A is closed under the binary operation of the **composition of functions**. Each element of the table corresponds to a function composition. For example, cell (2,3), i.e. row 2, column 3, reads as  $1/x \circ (1-x) = 1/_{1-x}$ . In *calculation*, we apply (1-x) first, i.e.  $x \rightarrow (1-x)$ , and then apply  $1/x$ , i.e.  $(1-x) \rightarrow 1/_{1-x}$ .

Q: How many *different* equivalence relations can be defined on a set of 4 distinct elements  $X = \{a,b,c,d\}$ ? A: Using the *theorem* that any partition on a set S defines an equivalence relation on S, we can say that the number of equivalence relations that can be defined on our set X is the number of ways that X can be **partitioned**. There are 15 partitions, listed as *follows*:  $\{a,b,c,d\}$ ;  $\{a\}\{b\}\{c\}\{d\}$ ;  $\{a\}\{bc\}\{d\}$ ;  $\{a\}\{bd\}\{c\}$ ;  $\{a\}\{cd\}\{b\}$ ;  $\{a\}\{bcd\}$ ;  $\{ab\}\{c\}\{d\}$ ;  $\{ab\}\{cd\}$ ;  $\{ac\}\{b\}\{d\}$ ;  $\{ac\}\{bd\}$ ;  $\{ad\}\{b\}\{c\}$ ;  $\{ad\}\{bc\}$ ;  $\{abc\}\{d\}$ ;  $\{abd\}\{c\}$ ; and  $\{acd\}\{b\}$ . Note that the **original** set  $\{a,b,c,d\}$  is also a partition.

Q: Let  $S = \mathbf{R} \setminus \{1\}$ , and define  $a*b = ab - a - b + 2$  for all  $a, b \in S$ . Show that “\*” is a closed binary operation on S. Show that “\*” is **associative**, and find its identity element. Show that every element of S has an **inverse** under “\*”. A: CLOSURE. We want to prove that all *elements*  $a*b$  are in the set S. This can be done by showing that we cannot have  $a*b = 1$  with  $a$  and  $b$  in S.

**Suppose** that  $a*b = 1$ . (The only way in which  $a*b \notin S$ ). Then  $ab - a - b + 2 = 1$ ;  $(a-1)(b-1) = 0$ ;  $a = 1$  or  $b = 1$ . But,  $1 \notin S$ , so *in this case*,  $a \notin S$  and/or  $b \notin S$ . Therefore, for all  $a$  &  $b$  in S, we also have  $a*b \in S$ . ASSOCIATIVITY. Calculate  $a*(b*c)$  and  $(a*b)*c$ , and show that they are *equal*. IDENTITY. We require that there *exists an*  $e \in S$  s.t.  $a*e = e*a = a$  for all  $a \in S$ .

So we *require*  $ae - a - e + 2 = a$ ; ...;  $(a-1)(e-2) = 0 \Rightarrow a = 1$  or  $e = 2 \in S$ . But  $a$  can **never** be 1 ( $1 \notin S$ ), so we must have  $e = 2$ . Now *check* that  $a*2 = a$  and  $2*a = a$ , e.g.  $2*a = 2.a - 2 - a + 2 = 2a - a = a$ . INVERSE. We require that for every *element*  $a \in S$ , there exists another element  $a^{-1} \in S$  s.t.  $a*a^{-1} = a^{-1}*a = e = 2$ . **Remember** to use “ $\in S$ ” where necessary.

So we *require*  $aa^{-1} - a - a^{-1} + 2 = 2$ ;  $a^{-1}(a-1) - a = 0$ ;  $a^{-1} = a/_{a-1}$ . This is **well defined** — the denominator can *never* be zero as  $a$  can never be 1 ( $1 \notin S$ ). **Checking** that  $a^{-1} \in S$  for all  $a \in S$ , if we let  $a/_{a-1} = 1$ , then  $a = a-1$ , which is clearly **not** true. Therefore, we will *always* have  $a/_{a-1} \in S$  for all  $a \in S$ . Now **check** that  $a*a^{-1} = a^{-1}*a = e$ .

## Permutation Groups

**Recall** that if  $X = \{1,2,\dots,n\}$ , then  $S_n$  is the symmetric group of *all permutations* (bijections) of X with the **group** operation of function composition. For example,  $(\begin{smallmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{smallmatrix}) \in S_3$  is the *bijection*  $(1 \rightarrow 2, 2 \rightarrow 1, 3 \rightarrow 3)$ .

**Cycle Notation**: If  $X = \{1,2,\dots,n\}$ , then  $(a_1 \dots a_k)$  is the *permutation* given by  $\{a_1 \rightarrow a_2, a_2 \rightarrow a_3, \dots, a_{k-1} \rightarrow a_k, a_k \rightarrow a_1\}$ ; and  $x \rightarrow x$  for all the *other*  $x \in X$ . We call  $(a_1 \dots a_k)$  a cycle of **length**  $k$ . For example, in  $S_3$ ,  $(\begin{smallmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{smallmatrix}) = (1\ 2\ 3)$  because  $1 \rightarrow 2, 2 \rightarrow 3$  and  $3 \rightarrow 1$ . **Others**:  $(\begin{smallmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{smallmatrix}) = (1\ 3\ 2)$ ;  $(\begin{smallmatrix} 1 & 2 & 3 \\ 2 & 3 & 2 \end{smallmatrix}) = (2\ 3)$ ;  $(\begin{smallmatrix} 1 & 2 & 3 \\ 3 & 2 & 3 \end{smallmatrix}) = (1\ 3)$ ; and  $(\begin{smallmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{smallmatrix}) = (1\ 2)$ .

**Notes:** (1) If  $\alpha$  is a cycle of length  $k$ , then  $\alpha^k = I$ , the identity permutation. (2) A cycle of length 2 is called a **transposition**. **Theorem:** Any permutation can be *expressed* as a product of disjoint cycles, i.e. no elements in *common*. The proof follows the line of the following example:

In  $({}^1_4 {}^2_8 {}^3_6 {}^4_7 {}^5_2 {}^6_3 {}^7_1 {}^8_5) \in S_8$ , follow the cycle of elements until it *closes*, e.g.  $1 \rightarrow 4 \rightarrow 7 \rightarrow 1$ , i.e.  $(1\ 4\ 7)$ . Now take the *next* unused number:  $2 \rightarrow 8 \rightarrow 5 \rightarrow 2$   $(2\ 8\ 5)$ . Next,  $3 \rightarrow 6 \rightarrow 1$   $(3\ 6)$ . Thus  $({}^1_4 {}^2_8 {}^3_6 {}^4_7 {}^5_2 {}^6_3 {}^7_1 {}^8_5) = (1\ 4\ 7)(2\ 8\ 5)(3\ 6)$ . Note that since they are **disjoint**, the order of composition is unimportant.

**Theorem:** Any permutation can be expressed as a *product* of transpositions (not usually disjoint; not unique). **Proof.** We need only treat a cycle  $(a_1\ a_2\ \dots\ a_k) = (a_1 a_2)(a_2 a_3)\dots(a_{k-1} a_k)$ , e.g.  $({}^1_3 {}^2_1 {}^3_4 {}^4_2) = (1\ 3\ 4\ 2) = (13)(3\ 4)(4\ 2)$ . **Check:** the *matrix* on the right

$$\begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 4 & 3 & 2 \\ 1 & 3 & 4 & 2 \\ 3 & 1 & 4 & 2 \end{pmatrix}$$

**Example:** Express  $(3\ 2\ 4)(1\ 4)(2\ 1\ 5)$  as a product of *disjoint cycles* of  $S_5$ . Constructing the matrix on the left, noting that we apply from **right to left**, the matrix is equivalent to  $({}^1_5 {}^2_3 {}^3_2 {}^4_1 {}^5_4)$ , and thus is  $(1\ 5\ 4)(2\ 3)$  [=  $(1\ 5)(5\ 4)(2\ 3)$ , expressing as *products* of transpositions]. Note that in examples such as  $({}^1_2 {}^2_1 {}^3_7 {}^4_3 {}^5_9 {}^6_6 {}^7_4 {}^8_8 {}^9_5)$ , this can be *expressed* as  $(1\ 2)(3\ 7\ 4)(5\ 9)$ . Note that when writing it out, you would do  $(1\ 2)(3\ 7\ 4)(5\ 9)(6)(8)$ , but as the 6 and the 8 are not affected, we just **leave** them out.

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 1 & 3 & 4 & 2 \\ 5 & 4 & 3 & 1 & 2 \\ 5 & 3 & 2 & 1 & 4 \end{pmatrix}$$

## Even and Odd Permutations

If a permutation  $\beta \in S_n$  can be expressed as the product of  $r$  **transpositions**, and  $r$  is even/odd, then we call  $\beta$  an *even/odd permutation*. **Notes:** (1) Although  $\beta$  can be expressed by different numbers of **transpositions**, their parity will be the same. (2) The product of an *even* permutation and an *even* permutation is an *even* permutation. Even and odd = odd; odd and even = odd; odd and odd = even. (Just adding **numbers** of transpositions). (3) The set of all even permutations in  $S_n$  forms a subgroup called the “*alternating group*”,  $A_n$ .

**Example:** In  $S_3$ ,  $\{I, (1\ 2\ 3) = (1\ 2)(2\ 3), (1\ 3\ 2) = (1\ 3)(3\ 2)\}$  are the *even* permutations, while the others are odd. So  $A_3 = \{I, (1\ 2\ 3), (1\ 3\ 2)\}$ .

7th March 2000

## Homomorphisms Between Groups

**Definition:** (1) A group *homomorphism* is a function  $\phi: G_1 \rightarrow G_2$  ( $G_1$  and  $G_2$  are groups) such that  $\phi(xy) = \phi(x)\phi(y)$  for all  $x, y \in G_1$ . (2) A *bijective* group homomorphism is called an isomorphism, denoted by  $G_1 \cong G_2$ . (Isomorphic groups are in effect **identical** as groups).

**Notes:** If  $\phi: G_1 \rightarrow G_2$  is a *group* homomorphism, then (a) if  $e_1$  &  $e_2$  are the respective identities in  $G_1$  and  $G_2$ , then  $\phi(e_1) = e_2$ . **Proof:**  $\phi(e_1) \cdot \phi(e_1) = \phi(e_1 e_1) = \phi(e_1) = e_2 \cdot \phi(e_1)$ . Multiply *both* sides by  $(\phi(e_1))^{-1}$  to obtain the result. (b)  $\phi(x^{-1}) = (\phi(x))^{-1}$  for all  $x \in G_1$ . **Proof:**  $\phi(x)\phi(x^{-1}) = \phi(xx^{-1}) = \phi(e_1) = e_2 = \phi(e_1) = \phi(x^{-1}x) = \phi(x^{-1}) \cdot \phi(x)$ .

The result follows by the *uniqueness* of  $(\phi(x))^{-1}$ . (c)  $\phi(G_1) = \{g_2: g_2 = \phi(g_1) \text{ for some } g_1 \in G_1\}$  is a **subgroup** of  $G_2$ . *Proof:* (i)  $\phi(G_1) \subseteq G_2$ .  $\checkmark$ . (ii) If  $a, b \in \phi(G_1)$ , then  $a = \phi(x)$  and  $b = \phi(y)$  for some  $x, y \in G_1$ ; and  $ab^{-1} = \phi(x)(\phi(y))^{-1} = \phi(x)\phi(y^{-1}) = \phi(xy^{-1}) \in \phi(G_1)$ .  $\checkmark$ .

**Example:** Let  $G_1 = C_4 = \{1, a, a^2, a^3\}$ , where  $a^4 = 1$ ; and let  $G_2 = C_2 = \{1, b\}$ , where  $b^2 = 1$ . Define  $\phi: G_1 \rightarrow G_2$  by  $1 \rightarrow 1$  and  $a^2 \rightarrow 1$ ;  $a$  and  $a^3 \rightarrow b$ . This gives a group **homomorphism**.

$G_1$	1	$a^2$	a	$a^3$
1	1	$a^2$	a	$a^3$
$a^2$	$a^2$	1	$a^3$	a
a	a	$a^3$	$a^2$	1
$a^3$	$a^3$	a	1	$a^2$

$G_2$	1	b
1	1	b
b	b	1

## Chapter 4: Lagrange's Theorem

**Definition:** Let  $G$  be a group, and let  $S$  be a subgroup of  $G$ . Let  $g \in G$ , and put  $gS = \{x \in G: x = gs \text{ for some } s \in S\}$ . We call  $gS$  a *left coset* of  $S$  in  $G$ . (We can also form right cosets).

**Notes:** (1)  $gS$  is **not usually** a subgroup; (2)  $g \in gS$  since  $g = g \cdot 1$ , where  $1 \in S$ .

**Theorem:** The *left cosets* of  $S$  in  $G$  form a partition of  $G$ . **Proof:** Define the relation  $\sim$  on  $G$  by  $g \sim h \Leftrightarrow gS = hS$ , with  $g, h \in G$ . (i) Reflexive:  $g \sim g$  since  $gS = gS$ . (ii) Symmetric:  $g \sim h \Rightarrow gS = hS \Rightarrow hS = gS \Rightarrow h \sim g$ . (iii) Transitive: If  $g \sim h$  and  $h \sim t$ , then  $gS = hS$  and  $hS = tS$ ,  $\Rightarrow gS = tS \Rightarrow g \sim t$ . Hence  $\sim$  is an equivalence relation as required.

**Note:** If  $X$  is a *left coset* of  $S$  in  $G$ , and if  $g \in X$ , then since  $g \in gS$  and the cosets *partition*  $G$ , we have  $X = gS$ . **Example:** Let  $G = U(\mathbb{Z}_{12}^*) = \{1, 5, 7, 11\}$ ; and let  $S = \{1, 5\}$  ( $5^2 = 1$ ). Then  $1 \cdot S = \{1 \cdot 1, 1 \cdot 5\} = \{1, 5\} = S = 5S$ ; (check:  $5S = \{5 \cdot 1, 5 \cdot 5\} = \{5, 1\}$ ); and  $7 \cdot S = \{7 \cdot 1, 7 \cdot 5\} = \{7, 11\} = 11S$ . Thus  $U(\mathbb{Z}_{12}^*)$  is partitioned into 2 cosets:  $1, 5 \mid 7, 11$ .

8th March 2000

### Examples

Let  $G = S_3 = \{I, (123), (132), (12), (13), (23)\}$ ; and let  $S = \{I, (123), (132)\}$  ( $= A_3$ ). We compute the *cosets* of  $S$  in  $G$ .  $I \cdot S = \{I, (123), (132)\} = (123)S = (132)S$ . **Now**  $(12)S = \{(12)I, (12)(123), (12)(132)\} = \{(12), (23), (13)\} = (\text{Looking at the } S_3 \text{ table}) = (23)S = (13)S$ . Thus  $S_3$  is partitioned into *two left cosets* by  $S$ :  $I, (123), (132)$ ; and  $(12), (23), (13)$ .

Let  $G = S_3$ ; and let  $S = \{I, (12)\}$ . ( $(12)^2 = I$ ). Find the *left cosets* of  $S$  in  $G$ , and give the partition of  $G$  they produce. Now  $I \cdot S = \{I, (12)\} = (12)S$ . Further,  $(123) \cdot S = \{(123)I, (123)(12)\} = \{(123), (13)\} = (13)S$ . **And**  $(132)S = \{(132)I, (132)(12)\} = \{(132), (23)\} = (23)S$ . Thus  $S_3$  is partitioned into 3 *left cosets* by  $S$ :  $I, (12)$ ;  $(123), (13)$ ; and  $(132), (23)$ .

### Lagrange's Theorem

If  $S$  is a *subgroup* of a finite group  $G$ , then the order of  $S$  *divides* the order of  $G$ , i.e.  $|S| \mid |G|$ . (The **cardinality** of  $S$  divides the **cardinality** of  $G$ ). **Proof:** The *left cosets* of  $S$  form a partition of  $G$ . We show that every coset has the same number of elements as  $S$ . For a fixed  $g \in S$ , define  $f_g: S \rightarrow gS$  by  $f_g(x) = gx$  for all  $x \in S$ . *Clearly*, by definition,  $f$  is surjective, i.e.  $f(S) = gS$ . Suppose that  $f_g(x_1) = f_g(x_2)$ , so that  $gx_1 = gx_2 \Rightarrow g^{-1}gx_1 = g^{-1}gx_2 \Rightarrow x_1 = x_2$ , So  $f$  is *injective*. By the Pigeon Hole principle,  $|f(S)| = |S|$ , i.e.  $|gS| = |S|$ .

**Corollary 1:** If  $G$  is a finite group of order  $n$ , and if  $x \in G$  is of order  $s$  ( $x^s = 1$ ), then  $s|n$ . **Proof:**  $x$  generates the cyclic subgroup  $\{1, x, x^2, \dots, x^{s-1}\}$  with  $s$  elements. **Corollary 2:** If  $G$  is a finite group of order  $n$ , then  $x^n = 1$  for all  $x \in G$ . **Note:** we are not saying that  $x$  is of order  $n$ , since the order of  $x$  is the smallest power of  $s$  for which  $x^s = 1$ . **Proof:** By corollary 1, if  $x$  is of order  $s$ , then  $s|n$ , i.e.  $n = rs$  for some  $r$ ;  $x^n = x^{rs} = (x^s)^r = 1^r = 1$ .

**Corollary 3:** If the order of  $G$  is a prime  $p$ , then  $G$  is a cyclic group of order  $p$ ,  $C_p$ . **Proof:** If  $x \in G$ , and if  $x \neq 1$ , then  $x$  generates a cyclic subgroup whose order divides  $p$ . But  $p$  is prime (its only factors are 1 and  $p$ ), and so this subgroup is  $G$  itself.

## Results in Number Theory

**Euler's Theorem:** Let  $n$  be a positive integer, then for all integers  $r$  relatively prime to  $n$ , (so that  $\gcd(r, n) = 1$ ),  $r^{\phi(n)} \equiv 1 \pmod{n}$ . **Proof:** Assume that  $r \in \mathbf{Z}_n^* = \{1, 2, \dots, n-1\}$ , then since  $r$  is relatively prime to  $n$ ,  $r \in U(\mathbf{Z}_n^*)$ , the invertible members of  $\mathbf{Z}_n^*$ ; and  $U(\mathbf{Z}_n^*)$  is a group under multiplication mod  $n$ . Further,  $U(\mathbf{Z}_n^*)$  is of order  $\phi(n)$ . Hence, by corollary 2,  $r^{\phi(n)} \equiv 1 \pmod{n}$ .

If  $r \notin \mathbf{Z}_n^*$ , we apply **Euclid's** algorithm, dividing  $r$  by  $n$  to give  $r = qn + r^*$ , with  $0 < r^* < n$ . (Note:  $r^* = 0 \Rightarrow \gcd(r, n) = 1$ ). Secondly,  $\gcd(r, n) = \gcd(r^*, n) = 1$ . Therefore,  $r \equiv r^* \pmod{n}$ , where  $r^* \in U(\mathbf{Z}_n^*)$  and  $r^{\phi(n)} \equiv (r^*)^{\phi(n)} \equiv 1 \pmod{n}$ .

**Corollary 1 (Fermat's Theorem):** Let  $p$  be a prime number, then for all integers  $r$  relatively prime to  $p$ , (i.e.  $p \nmid r$ ),  $r^{p-1} \equiv 1 \pmod{p}$ . **Proof:** If  $p$  is prime, then  $\phi(p) = p-1$ . **Corollary 2 (The general form of Fermat's Theorem):** Let  $p$  be a prime number, then for all integers  $r$ ,  $r^p \equiv r \pmod{p}$ . **Proof:** If  $p \nmid r$ , then the result follows by multiplying by  $r$  in corollary 1. If  $p | r$ , then  $r$  is a multiple of  $p$ , and  $r^p \equiv r \equiv 0 \pmod{p}$ .

**Examples:** We can use these results to rapidly reduce powers to members of  $\mathbf{Z}_m^*$ , provided the conditions are satisfied. (i)  $2^{100}$  in  $\mathbf{Z}_{17}^*$ . Since 17 is prime and 2 is clearly not a multiple of 17, we use Fermat's Theorem with  $p = 17$  and  $r = 2$ . So  $2^{16} \equiv 1 \pmod{17}$ . Repeated application gives  $2^{100} \equiv (2^{16})^6 \cdot 2^4 \equiv 16 \pmod{17}$ .

(ii)  $15^{110}$  in  $\mathbf{Z}_{26}^*$ . Since 15 is relatively prime to 26, we can use Euler's Theorem with  $r = 15$  and  $n = 26$ , where  $\phi(26) = \phi(2 \times 13) = (2-1)(13-1) = 12$ , to give  $15^{12} \equiv 1 \pmod{26}$ . Now  $15^{110} \equiv (15^{12})^9 \cdot 15^2 \equiv 225 \equiv 17 \pmod{26}$ . (iii)  $16^{55}$  in  $\mathbf{Z}_{27}^*$ . 16 and 27 are relatively prime, so using Euler's theorem with  $r = 16$  and  $n = 27$ , and knowing that  $\phi(27) = \phi(3^3) = 3^3 - 3^2 = 18$ , we get  $16^{18} \equiv 1 \pmod{27}$ ;  $16^{55} \equiv (16^{18})^3 \cdot 16^1 \equiv 16 \pmod{27}$ .

14th March 2000

## Useful Result

Let  $l$  be the least common multiple of  $m$  and  $n$ , then  $a \equiv b \pmod{m}$  and  $a \equiv b \pmod{n}$  both imply that  $m | (a-b)$  and  $n | (a-b)$ , which imply that  $l | (a-b)$ , which implies that  $a \equiv b \pmod{l}$ . So, for example, if  $a \equiv b \pmod{10}$ , then  $a \equiv b \pmod{5}$  and  $a \equiv b \pmod{2}$ . **Theorem:** In numbers written to base 10 (i.e. as usual), a number and its fifth power have the same final digit, i.e.  $r^5 \equiv r \pmod{10}$  for all  $\mathbf{Z}$ . **Example:**  $32 \pmod{10} \equiv 2$ ;  $2^5 \equiv 2 \pmod{10}$ .

**Proof:** By the above, we need only *show* that  $r^5 \equiv r \pmod{5}$  and  $r^5 \equiv r \pmod{2}$ , since the *lcm* of 5 and 2 is 10. However, by the general form of Fermat's theorem,  $r^5 \equiv r \pmod{5}$  and  $r^2 \equiv r \pmod{2}$ , and we can use *this* to get  $r^5 \equiv (r^2)^2 \cdot r \equiv (r^2)r \equiv r \cdot r \equiv r \pmod{2}$ .

**Example:** Find the last 2 *digits* of  $13^{41}$  (to base 10). Here, we need to **find**  $13^{41} \pmod{100}$ . We can use *Euler's* theorem, since 13 is relatively prime to 100, i.e.  $13^{\phi(100)} \equiv 1 \pmod{100}$ . Now  $\phi(100) = (5^2-5)(2^2-2) = 40$ . Hence  $13^{40} \equiv 1 \pmod{100}$ ;  $13^{41} \equiv (13^{40})13 \equiv 13 \pmod{100}$ . Q: Find the *last two digits* of  $7^{82}$ . Since 7 is **relatively prime** to 82, we can use Euler's theorem,  $7^{\phi(82)} \equiv 1 \pmod{100}$ ;  $7^{40} \equiv 1 \pmod{100}$ . So  $7^{82} \equiv (7^{40})(7^{40})7^2 \equiv (1)(1)49 \equiv 49 \pmod{100}$ .

Q: *Show that*  $r^5 \equiv r \pmod{30}$  for all  $r \in \mathbf{Z}$ . Since  $30 = 2 \times 3 \times 5$  (the *lcm* of 2, 5 and 3), we need only show that  $r^5 \equiv r \pmod{5}$ ;  $r^5 \equiv r \pmod{3}$ ; and  $r^5 \equiv r \pmod{2}$ . By the *general* form of Fermat's Theorem, we have  $r^5 \equiv r \pmod{5}$ ;  $r^3 \equiv r \pmod{3}$ ; and  $r^2 \equiv r \pmod{2}$ . **Now**  $r^5 \equiv (r^2)^2 \cdot r \equiv r^2 \cdot r \equiv r \cdot r \equiv r^2 \equiv r \pmod{2}$ ; and  $r^5 \equiv (r^3)(r^2) \equiv r \cdot r^2 \equiv r^3 \equiv r \pmod{3}$ .

## R.S.A. Coding

**RSA Coding Theorem:** (i) Let  $n = pq$ , where  $p$  and  $q$  are *distinct* primes. (ii) Let  $e$  and  $d$  be integers such that  $ed \equiv 1 \pmod{\phi(n)}$ . It follows that  $r^{ed} \equiv r \pmod{n}$  for all  $r \in \mathbf{Z}$ . **Proof.** We first show that  $r^{ed} \equiv r \pmod{p}$  for all  $r \in \mathbf{Z}$ . (i) *Assume that*  $p \nmid r$  (i.e.  $r$  is *relatively prime* to  $p$ ). Since  $ed \equiv 1 \pmod{\phi(n)}$ , then  $ed = k\phi(n)+1$  for *some*  $k \in \mathbf{Z}$ .

Then  $r^{ed} \equiv (r^{\phi(n)})^k \cdot r \pmod{p}$ ;  $r^{ed} \equiv (r^{(p-1)(q-1)})^k \cdot r \equiv (r^{p-1})^{(q-1)k} \cdot r$ . **But**  $r^{p-1} \equiv 1 \pmod{p}$  by *Fermat's Theorem*, so  $r^{ed} \equiv (1)^{(q-1)k} \cdot r \equiv r \pmod{p}$ . (ii) **Assume that**  $p \mid r$ , then  $r$  is a *multiple* of  $p$ , and  $r^{ed} \equiv r \equiv 0 \pmod{p}$ . Hence  $r^{ed} \equiv r \pmod{p}$  for all  $r \in \mathbf{Z}$ , and *similarly*  $r^{ed} \equiv r \pmod{q}$  for all  $r \in \mathbf{Z}$ . Hence *since*  $n = pq$  is the *lcm* of  $p$  and  $q$ , then  $r^{ed} \equiv r \pmod{n}$  for all  $r \in \mathbf{Z}$ .

## Assignment 3: Set 15/3; In 22/3; Back 22/3

Q: Find a *generator* for the multiplicative group  $\mathbf{Z}_{17}^* = \{1, 2, \dots, 16\}$ . List all elements as powers of this generator. Find all *other* possible generators of the group. A: Using the theorem "If  $p$  is a prime, then  $\mathbf{Z}_p^*$  is a *cyclic group* of order  $(p-1)$  under multiplication mod  $p$ ", we can say that because 17 is prime, then  $\mathbf{Z}_{17}^*$  is a *cyclic group* of *order* 16.

A generator of this group **must** be of order 16, so we need  $a^{16} \equiv 1 \pmod{17}$  and  $a^n \not\equiv 1 \pmod{17}$  for  $1 \leq n \leq 15$ . 2 is **not** a generator as  $2^8 = 256 = (15 \times 17) + 1 \equiv 1 \pmod{17}$ . Suppose that 3 is a generator of  $\mathbf{Z}_{17}^*$ . Let us find the *order* of 3:  $3^1 \equiv 3 \pmod{17}$ ;  $3^2 \equiv 9 \pmod{17}$ ;  $3^3 = 27 \equiv 10 \pmod{17}$ ;  $3^4 = 81 = (4 \times 17) + 13 \equiv 13 \pmod{17}$ ;  $3^5 = 243 = (14 \times 17) + 5 \equiv 5 \pmod{17}$ ; ...; *until*  $3^{16} = 43046721 = (2532160 \times 17) + 1 \equiv 1 \pmod{17}$ .

As  $3^{16} \equiv 1 \pmod{17}$ , and  $3^n \not\equiv 1 \pmod{17}$  for  $1 \leq n \leq 15$ , then 3 is of *order* 16, and is thus a **generator** of  $\mathbf{Z}_{17}^*$ . Using the above (*incomplete*) information, we can list all elements of  $\mathbf{Z}_{17}^*$  as *powers* of 3:  $1 \pmod{17} \equiv 3^{16}$ ;  $2 \pmod{17} \equiv 3^{14}$ ;  $3 \pmod{17} \equiv 3^1$ ; and *so on*.

All other **possible** generators of the group are given by  $3^q$ , where  $q$  is *relatively prime to 16*. As  $16 = 2^4$ , the numbers relatively prime to 16 are the **odd** numbers. Therefore,  $q = 1, 3, 5, 7, 9, 11, 13$  and  $15$ , and we have *generators*  $3^1 \equiv 3 \pmod{17}$ ;  $3^3 \equiv 10 \pmod{17}$ ;  $3^5 \equiv 5 \pmod{17}$ ;  $3^7 \equiv 11 \pmod{17}$ ;  $3^9 \equiv 14 \pmod{17}$ ;  $3^{11} \equiv 7 \pmod{17}$ ;  $3^{13} \equiv 12 \pmod{17}$ ; and  $3^{15} \equiv 6 \pmod{17}$ , i.e. the *generators* of  $\mathbf{Z}_{17}^*$  are 3, 5, 6, 7, 10, 11, 12 and 14. We have 8 *generators*: check:  $\phi(16) = \phi(2^4) = 2^4 - 2^3 = 16 - 8 = 8$ .

**Q:** Find the order of **every** element of the multiplicative group  $U(\mathbf{Z}_{20}^*) = \{1, 3, 7, 9, 11, 13, 17, 19\}$ . Hence show that this group is *not* cyclic. **A:** The *order* of the group is 8 as it has 8 elements. To prove that the group is **not** cyclic, we must show that if  $a$  is an element of  $U(\mathbf{Z}_{20}^*)$ ,  $a$  does not have order 8. Let us find the order of **each** element in  $U(\mathbf{Z}_{20}^*)$ . (1)  $1^1 \equiv 1 \pmod{20}$ , so 1 is of order 1. (3)  $3^1 \equiv 3 \pmod{20}$ ;  $3^2 \equiv 9 \pmod{20}$ ;  $3^3 \equiv 27 \equiv 7 \pmod{20}$ ;  $3^4 \equiv 81 \equiv 1 \pmod{20}$ , so 3 is of *order* 4. And so on for (7), (9), (11), (13), (17) and (19). Because **all** the elements of the group are of orders 1, 2 or 4, and we have no elements of order 8, then there are no *generators*, and thus the group is **not** cyclic.

**Q:** Find the last **three** digits of  $13^{41210}$ . **A:** If we need the last 3 digits, we need to *work modulo 1000*. Since 13 is relatively prime to 1000 ( $\gcd(13, 1000) = 1$ ), we can use **Euler's** Theorem to say that  $13^{\phi(1000)} \equiv 1 \pmod{1000}$ . Now  $\phi(1000) = \phi(2^3 \cdot 5^3) = (2^3 - 2^2)(5^3 - 5^2) = 400$ , so  $13^{400} \equiv 1 \pmod{1000}$ .

Now as  $41210 = (103 \times 400) + 10$ , then  $13^{41210} = (13^{400})(13^{400}) \dots (13^{400})(13^{10})$  [**103 times**], and so  $13^{41210} \equiv (13^{400})(13^{400}) \dots (13^{400})(13^{10}) \pmod{1000} \equiv (1)(1) \dots (1)(13^{10}) \pmod{1000} \equiv 13^{10} \pmod{1000}$ . Now as  $13^2 \equiv 169 \pmod{1000}$ , we have  $13^4 \equiv 169^2 \equiv 28561 \equiv 561 \pmod{1000}$ ; and  $13^8 \equiv 561^2 \equiv 314721 \equiv 721 \pmod{1000}$ ; so  $13^{10} \equiv 13^8 \cdot 13^2 \equiv 721 \cdot 169 \equiv 121849 \equiv 849 \pmod{1000}$ . *Therefore,  $13^{41210} \equiv 849 \pmod{1000}$ , and the **final** three digits of  $13^{41210}$  are 8, 4 and 9.*

**Q:** Show that for all  $n \in \mathbf{Z}$ ,  $n^{13} \equiv n \pmod{2730}$ . **A:** Since  $2730 = 2 \times 3 \times 5 \times 7 \times 13$ , and  $13 = 1 \times 13$ , the l.c.m. of 13 and 2730 is  $2 \times 3 \times 5 \times 7 \times 13 = 2730$ . So to prove the above, we need only show that the *following are true*:  $n^{13} \equiv n \pmod{2}$ ;  $n^{13} \equiv n \pmod{3}$ ;  $n^{13} \equiv n \pmod{5}$ ;  $n^{13} \equiv n \pmod{7}$ ; and  $n^{13} \equiv n \pmod{13}$ . The final expression comes *straight from* and is **proved by** the general form of Fermat's theorem. From the same theorem, we can obtain the following:

$n^2 \equiv n \pmod{2}$  (---(1));  $n^3 \equiv n \pmod{3}$  (---(2));  $n^5 \equiv n \pmod{5}$  (---(3)); and  $n^7 \equiv n \pmod{7}$  (---(4)). Now, *using* (1),  $n^{13} = n(n^6)^2 \equiv n \cdot n^6 \equiv n(n^3)^2 \equiv n \cdot n^3 \equiv n^4 \equiv (n^2)^2 \equiv n^2 \equiv n \pmod{2}$ . Using (2),  $n^{13} = n^3 \cdot n^3 \cdot n^3 \cdot n^3 \cdot n \equiv n \cdot n \cdot n \cdot n \cdot n \equiv n^3 \cdot n^2 \equiv n \cdot n^2 \equiv n^3 \equiv n \pmod{3}$ . Using (3),  $n^{13} = n^5 \cdot n^5 \cdot n^3 \equiv n \cdot n \cdot n^3 \equiv n^5 \equiv n \pmod{5}$ . And using (4),  $n^{13} = n^7 \cdot n^6 \equiv n \cdot n^6 \equiv n^7 \equiv n \pmod{7}$ . We therefore have all the *relevant* results, and we can **say** that  $n^{13} \equiv n \pmod{2730}$  for all  $n \in \mathbf{Z}$ .

15th March 2000

## Public Key Coding

Suppose that *person "R"* intends to receive **coded** messages in such a way that (1) everyone knows how to encode a message to "R"; (2) **no one but "R"** can decode a message, i.e. the key to encoding is "*public*", but even so, without special extra knowledge known only to "R", you cannot **decode** any messages.

**Using R.S.A.** (1) Let letters be converted into *numbers* by, say, A→01, B→02, ..., Z→26 — e.g. HELLO → 0805121215. (2) “R” chooses *primes* p and q, and chooses e relatively prime to  $\phi(n)$ , so that  $e^{-1} \equiv d \pmod{\phi(n)}$  exists, i.e. “R” can *compute* d such that  $ed \equiv 1 \pmod{\phi(n)}$ . (3) “R” makes public the *numbers n and e*, but keeps d **secret**. (p and q are therefore secret).

(4) To encode a message *number r*, we compute  $r^e \equiv M \pmod{n}$ . (5) To decode M, “R” just needs to compute  $M^d \equiv r^{ed} \equiv r \pmod{n}$ . (6) The important thing is that for *large* n (i.e. p and q are large primes), it is thought to be impossible to compute  $\phi(n)$  (and so d) without knowledge of the prime *decomposition* for  $n = pq$ . (7) For *practical purposes*, the message number r needs to be in the range  $0 \leq r \leq (n-1)$ , and the message has to be broken down into blocks of **this** size.

**Example** (We’ll illustrate using *small* numbers). Let p = 3 and q = 11, so that  $n = pq = 33$ ; and  $\phi(n) = (3-1)(11-1) = 20$ . Choose e *relatively prime* to 20, say e = 7, and so d = 3. ( $7 \times 3 \equiv 21 \equiv 1 \pmod{20}$ ). Let the message be “SEE”. We encipher 2 *digits* at a time. The public key is n = 33 and e = 7. Now SEE → 19, 05, 05. Enciphering, we need to *compute*  $19^7 \pmod{33}$ .

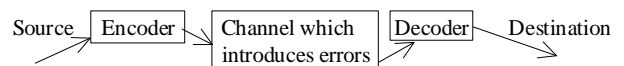
A useful device is to break this down into *powers of 2* —  $7 = 4+2+1$ , and to compute, reducing mod 33 at each stage:  $19^2 \equiv 31 \pmod{33}$ ;  $(19^2)^2 \equiv (31)^2 \equiv 4 \pmod{33}$ . So  $19^7 \equiv (19^4)(19^2)19 \equiv 4 \cdot 31 \cdot 19 \equiv 13 \pmod{33}$ . *Similarly*,  $5^7 \equiv 14 \pmod{33}$ , so the coded message is 13, 14, 14. To decipher, we must compute  $13^3 \pmod{33}$ , etc. We get back:  $13^3 \equiv 19 \pmod{33}$  (**OK**),  $14^3 \equiv 5 \pmod{33}$ . (**OK**).

Q: p = 3; q = 41; n = pq = 123;  $\phi(n) = (41-1)(3-1) = 80$ ; and e = 27 is an *RSA public key coding system* (with public key n = 123, e = 27). Encipher the message “GO”, one letter at a time. Check by decoding with the **appropriate** value of d. A: We want d s.t.  $ed \equiv 1 \pmod{80}$ ;  $27 \times 3 = 81 \equiv 1 \pmod{80}$ . So d = 3.

GO → 07, 15. We now *want*  $7^{27} \pmod{123}$ . Calculate powers of 7:  $7^2 \equiv 49 \pmod{123}$ ;  $7^4 \equiv 49^2 \equiv 64 \pmod{123}$ ;  $7^8 \equiv 37 \pmod{123}$ ;  $7^{16} \equiv 16 \pmod{123}$ ; and  $7^{24} \equiv 16 \cdot 37 \equiv 100 \pmod{123}$ . So  $7^{27} \equiv 100 \cdot 49 \cdot 7 \equiv 106 \pmod{123}$ . We now *want*  $15^{27} \pmod{123}$ . Calculate powers of 15:  $15^2 \equiv 102 \pmod{123}$ ;  $15^4 \equiv 72 \pmod{123}$ ; and *so on* to get  $15^{27} \equiv 48 \pmod{123}$ . So the **coded** message is 106, 48. To decode, *compute*  $106^3 \pmod{123} \equiv 7 \pmod{123}$  (✓) and  $48^3 \pmod{123} \equiv 15 \pmod{123}$  (✓).

## Chapter 5: The Theory of Error Correcting Codes

Suppose that we are sending *messages* in binary (in 0’s and 1’s) along a channel which introduces errors into the message. In order to increase the reliability, we change our original message by coding it in some way so that we can (1) **Detect** Errors; (2) **Correct** Errors.



**Definition:** Let vector  $\underline{a} = (a_1, a_2, \dots, a_m) \in \mathbf{Z}_2^m$  be a *message word*. ( $\mathbf{Z}_2 = \{0, 1\}$ ). Example:  $\underline{a} = (1, 1, 0, \dots, 1, 0)$  contains m “*bits*” of information. A **code** is a function which takes  $\underline{a} \in \mathbf{Z}_2^m$  to an *element*  $\underline{b} \in \mathbf{Z}_2^n$  ( $\underline{a} \mapsto \underline{b}$ ), where  $n \geq m$  and  $\underline{b}$  is a “code word”. (We assume that *different* messages give different code words, i.e. the code is injective, and  $\underline{b}$  is longer than  $\underline{a}$ ).

The *extra information* in  $\underline{b}$  can be used for (1) error **detection**; (2) error **correction**. The above code is called “an  $(m,n)$  code”. The information rate of the code is  $\frac{m}{n} \leq 1$ . **Examples:** (1) Parity Check Code. Define the code by  $\underline{a} = (a_1, \dots, a_m) \mapsto (a_1, \dots, a_m, a_{m+1}) = \underline{b}$ , where  $a_{m+1} \equiv \sum_{i=1}^m a_i \pmod{2}$ , i.e.  $a_{m+1} = 0$  if there are an *even* number of 1’s, and  $a_{m+1} = 1$  if there is an odd number of 1’s. Hence the **parity** of  $\underline{b}$  is always even:  $\sum_{i=1}^{m+1} a_i \equiv 0 \pmod{2}$ . This is an  $(m, m+1)$  code, with *information rate*  $\frac{m}{m+1}$ .

**Examples:**  $(1,1) \mapsto (1,1,0)$ ;  $(0,1) \mapsto (0,1,1)$ , a  $(2,3)$  parity check code. Now *transmit*  $\underline{b}$ . If the *received* code word  $\underline{r} = (r_1, \dots, r_{m+1})$  is such that  $\sum_{i=1}^{m+1} r_i \equiv 1 \pmod{2}$ , then there has been an *odd number* of errors. If  $\sum_{i=1}^{m+1} r_i \equiv 0 \pmod{2}$ , then there are no *errors*, or an even number of errors. **Note:** This procedure does not detect *even* numbers of errors, and does not *correct* any errors.

**Example 2:** The Triple Repeat Code:  $\underline{a} = (a_1, \dots, a_m) \mapsto (a_1, \dots, a_m, a_1, \dots, a_m, a_1, \dots, a_m) = \underline{b}$ . This is an  $(m, 3m)$  code with *information rate*  $= \frac{1}{3}$ . If we now *transmit*  $\underline{b}$ , and if there is no more than **1** error in repetition, then we will be able to detect and correct it.

**The space  $\mathbf{Z}_2^m$ .** **Definitions:** (i) If  $\underline{a} = (a_1, \dots, a_m) \in \mathbf{Z}_2^m$ , then the *weight* of  $\underline{a}$  is  $w(\underline{a}) = \sum_{i=1}^m a_i$ , i.e. the *number of 1’s* in  $\underline{a}$ . (ii) If  $\underline{a}, \underline{b} \in \mathbf{Z}_2^m$ , then the *distance* between  $\underline{a}$  and  $\underline{b}$  is  $d(\underline{a}, \underline{b}) = w(\underline{a} - \underline{b})$ . (Vector subtraction in  $\mathbf{Z}_2^m$ ). For example,  $w(10110) = 3$ ;  $w(000) = 0$ ; and  $d((011010), (110011))$  as calculated in the *diagram* is 3. (Recall that **subtraction** and **addition** are the same in  $\mathbf{Z}_2^m$ ).

Here,  $d(\underline{a}, \underline{b}) = w(\underline{a} - \underline{b}) = w(\underline{a} + \underline{b}) =$  the number of places where  $\underline{a}$  and  $\underline{b}$  *differ*. (iii) If we encode  $\underline{a} \in \mathbf{Z}_2^m$  to be  $\underline{b} \in \mathbf{Z}_2^n$ , and then *transmit*  $\underline{b}$ , with **received** word  $\underline{r}$ , we call  $\underline{e} = \underline{r} - \underline{b}$  the *error vector*, with  $w(\underline{e}) = w(\underline{r} - \underline{b}) = w(\underline{r} + \underline{b}) = d(\underline{r}, \underline{b}) =$  the number of *places* where  $\underline{r}$  and  $\underline{b}$  differ, the number of errors in  $\underline{r}$ .

21st March 2000

## Probabilities

Assume that for every *transmitted digit*, we have the same probability of **correct** receipt  $p$ . Then  $q = 1 - p =$  the probability of an **error** in any one digit. Assume that errors in different digits are independent, so that the fact that a digit is *unaffected* has no relevance to the fate of other digits. Let the code word  $\underline{b} \in \mathbf{Z}_2^n$  be transmitted, and let  $\underline{r} \in \mathbf{Z}_2^n$  be the *received* word.

Let  $q_w$  be the probability that the error vector  $\underline{e} = \underline{r} - \underline{b}$  is of weight  $w$  (i.e. there are  $w$  *errors* in  $\underline{r}$ ). **Theorem:**  $q_w = \binom{n}{w} p^{n-w} q^w$ . **Proof:** The probability of  $w$  *errors and*  $n-w$  *correct bits* in some particular order is precisely  $p^{n-w} q^w$ . The number of different **orders** for the  $w$  errors and  $n-w$  correct bits is  $\binom{n}{w}$ . Hence  $q_w = \binom{n}{w} p^{n-w} q^w$ . (This is the probability of  $w$  “*successes*” in a binomial distribution with probability of **success**  $q$  (the error)).

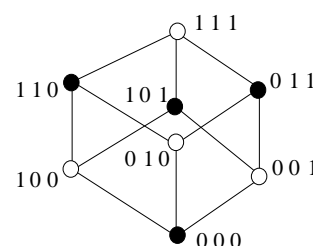
**Q:** In a  $(3,4)$  parity check, let the *message words*  $\underline{a}$  be  $(0,1,1)$  and  $(1,0,0)$ . Give the appropriate *code word*  $\underline{b}$  in each case. Give the **weight** of all the individual message and code words. Give the **distance** between the message words and the distance between the code words. If the probability of correct *receipt* of a single digit  $p$  is 0.9, what is the probability of exactly **2** errors in a received word  $\underline{r}$ ?

A:  $(0,1,1) \mapsto (0,1,1,0)$ ;  $(1,0,0) \mapsto (1,0,0,1)$ . Now  $w(0,1,1) = 2$ ;  $w(0,1,1,0) = 2$ ;  $w(1,0,0) = 1$ ; and  $w(1,0,0,1) = 2$ . For the *message* words,  $d(\underline{a}, \underline{b}) = w(1,1,1) = 3$ . For the *code* words,  $d(\underline{a}, \underline{b}) = w(1,1,1,1) = 4$ . Now using  $q_w = \binom{n}{w} p^{n-w} q^w$  with  $n = 4$ ,  $w = 2$ , and  $p=0.9$ , we get  $q_2 = \binom{4}{2} 0.9^2 0.1^2 = 6 \times 0.81 \times 0.01 = 0.0486$ .

## Standard Decoding Procedure

(*Maximum Likelihood Decoding; Nearest Neighbour Decoding*). We **encode**  $\underline{a} \in \mathbf{Z}_2^m$  by a distinct *code word*  $\underline{b} \in \mathbf{Z}_2^n$  (where  $n \geq m$ ). Hence  $\mathbf{Z}_2^n$  contains  $|\mathbf{Z}_2^m| = 2^m$  code words. (i) If the *received* word  $\underline{r}$  is one of the  $2^m$  code words in  $\mathbf{Z}_2^n$ , then we assume it is *correct*. (ii) If  $\underline{r}$  is one of the  $2^n - 2^m$  *other* words in  $\mathbf{Z}_2^n$ , then we know that there is an **error** vector  $\underline{e} = \underline{r} - \underline{b}$ , and we decode  $\underline{r}$  as the code word  $\underline{c}$  which *minimises* the distance  $d(\underline{r}, \underline{c})$ , i.e. we take the *nearest* code word to  $\underline{r}$ . Note: there may be **more** than one such  $\underline{c}$ , in which case we must *choose*.

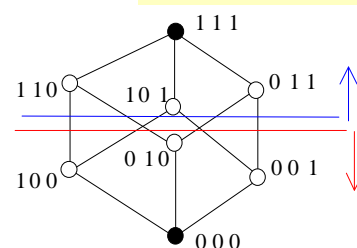
**Example 1:** *Parity Check Code*,  $m = 2$ ,  $n = 3$ . We have message words  $(0,0)$ ,  $(0,1)$ ,  $(1,0)$ , and  $(1,1)$ , and they go to *code words*  $(0,0,0)$ ,  $(0,1,1)$ ,  $(1,0,1)$ , and  $(1,1,0)$  respectively. In the diagram shown of  $\mathbf{Z}_2^3$ , the **filled in** circles are *code words*, while the **empty** circles are *non-code words*. We join all words which are at a distance of 1 apart.



(i) If the **received** word is a *code word*, we decode as above, e.g.  $0\ 1\ 1$  decodes as  $0\ 1$ . (ii) If  $\underline{r}$  is **not** a code word, then we choose a code word a distance 1 *from* it, e.g.  $1\ 0\ 0 \mapsto 1\ 0\ 1 \mapsto 1\ 0\ 1$  (**Note:** *Choice* of 3 possibilities: can have  $100 \mapsto 110 \mapsto 11$  or  $100 \mapsto 000 \mapsto 00$  as well). Every non-code word has a code word within *distance 1* of it (but it is not unique). We detect every error of **weight 1**, but miss every error of **weight 2**.

**Example 2:** *Triple Repeat Code* ( $m = 1$ ,  $n = 3$ ). Consider that we have message words 0 and 1 going to code words 000 and 111. Here, every *non-code* word has a unique nearest code word at a distance 1 from it. Thus, we detect any error of **weight 1** or **weight 2**; (an error of **weight 3** would not be detected); and correct all errors of **weight 1**. (Errors of weight 2 go the **wrong** way). For example,  $1 \mapsto 111 \rightsquigarrow 110 \mapsto 111 \mapsto 1$  (**OK**). And  $1 \mapsto 111 \rightsquigarrow 010 \mapsto 000 \mapsto 0$  (**WRONG**).

22nd March 2000



## Probabilities for the Triple Repeat Code

The probability that each of the 3 *bits* in the code word are transmitted correctly is  $p^3$ . The probability that an error of **weight 1** occurs is  $3p^2q$ ; of **weight 2** is  $3pq^2$ ; and of **weight 3** is  $q^3$ . Hence the probability of *correctly decoding the word* is  $p^3 + 3p^2q$ , and of *detecting an error* is  $p^3 + 3p^2q + 3pq^2$ . In general, for any Triple Repeat Code with  $m$ -bit words (and  $3m$ -bit code-words), the probability of correctly **decoding** a word is  $(p^3 + 3p^2q)^m$ , since the probability of *each bit* being correct is  $p^3 + 3p^2q$ . **Definition:** The *minimum distance* of a code is the minimum distance between distinct code words of the code. Exercises 1 and 2 (above): the minimum distances are 2 and 3 respectively. **Theorem:** (1) We can detect all *errors* of weight  $\leq k$  iff the **minimum distance** of the code is  $\geq k+1$ . (2) We can *correct* all errors of weight  $\leq k$  iff the minimum distance of the code is  $\geq 2k+1$ . **Proof:** see the text book.

In *Example 1*, we detect all errors of weight 1 (minimum distance 2) but can say **nothing** about correction. In *Example 2*, we detect all errors of weights 1 and 2, and correct all errors of weight 1. (Minimum distance = 3).

## Matrix Codes

We may be able to obtain the *coding*  $\underline{a} \mapsto \underline{b}$  by multiplying by a *matrix* (c.f. **Hill** codes).

**Definition:** The  $m \times n$  matrix  $E$  (such that  $\underline{a} \mapsto \underline{a}E = \underline{b}$ ) is called the *encoding* matrix of the matrix code. Note: Not all codes are matrix codes. **Example 1:** (*Parity* check, with  $00 \mapsto 000$ ,  $01 \mapsto 011$ ,  $10 \mapsto 101$ , and  $11 \mapsto 110$ ). We can get  $E$  by taking the images of the **basis**  $\{(10), (01)\}$  of  $\mathbf{Z}_2^2$ , i.e.  $E = \begin{pmatrix} 1 & 0 \\ 0 & 1 \\ 1 & 1 \end{pmatrix}$ . Check:  $(11) \mapsto (11)\begin{pmatrix} 1 & 0 \\ 0 & 1 \\ 1 & 1 \end{pmatrix} = (110)$ , OK. **Example 2:** *Triple Repeat*, with  $m = 1$  and  $n = 3$ :  $E = (111)$ .

**Standard Form.** We say that  $\underline{a} \mapsto \underline{a}E = \underline{b}$  is in *standard form* if  $\underline{a} \mapsto (a_1, a_2, \dots, a_m, \dots)$ , i.e.  $b_i = a_i$  (for  $i = 1, \dots, m$ ) **and**  $E = (I_m, P)$ , where  $I_m$  is an  $m \times m$  *identity matrix*, and  $P$  is an  $m \times (n-m)$  matrix. From **Example 1**,  $E = (I_2, P)$ , where  $P = \begin{pmatrix} 1 \\ 1 \end{pmatrix}$ . Q: Give the encoding matrix  $E$  for the (3,4) parity check code in **standard form**. A: We need *only know* that  $100 \mapsto 1001$ ,  $010 \mapsto 0101$ , and  $001 \mapsto 0011$  to get  $E$  as shown on the *right* in standard form. Note that  $E = (I_3, P)$ , where  $P = \begin{pmatrix} 1 \\ 1 \\ 1 \end{pmatrix}$ .

$$E = \begin{pmatrix} 1 & 0 & 0 & 1 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 \end{pmatrix}$$

## Group Codes (Linear Codes)

A *group code* is a code in which the code words of  $\mathbf{Z}_2^n$  form a group (under addition).

**Theorem:** A *matrix* code is a group code. **Proof:** The code  $\mathbf{Z}_2^m \rightarrow \mathbf{Z}_2^n$  defined by  $\underline{a} \rightarrow \underline{a}E$  is a *group homomorphism* of the additive groups  $\mathbf{Z}_2^m$  and  $\mathbf{Z}_2^n$ , for if  $\underline{a}_1, \underline{a}_2 \in \mathbf{Z}_2^m$ , then  $(\underline{a}_1 + \underline{a}_2)E = \underline{a}_1E + \underline{a}_2E$ . Hence the *image*, which is the set of code words  $C$ , forms a subgroup of  $\mathbf{Z}_2^n$ .

**Theorem:** The *minimum distance* of a group is the minimum weight of the non-zero code words. **Proof:** we show that every distance value which occurs is also the *weight* of some code word  $d(\underline{c}_1, \underline{c}_2) = w(\underline{c}_1 - \underline{c}_2) = w(\underline{c}_1 + \underline{c}_2)$ , but since the *code words* form a group,  $\underline{c}_1 + \underline{c}_2 = \underline{c}_3$  for some **other** code word i.e.  $d(\underline{c}_1, \underline{c}_2) = w(\underline{c}_3)$ . On the other hand, *every weight value* which occurs also occurs as a distance value for two code words:  $w(\underline{c}_1) = d(\underline{0}, \underline{c}_1)$ , where  $\underline{0}$  is the *identity* element of the group of code words.

## Decoding Tables

Take an  $(m, n)$  *matrix code*. Recall that in decoding, we take the **nearest** code word to the received word  $\underline{r}$  (but there may be *several* code words equidistant from  $\underline{r}$ ). **Standard Decoding Table** (S.D.T.). The code words  $C$  form a *subgroup* of the additive group  $\mathbf{Z}_2^n$ . Hence the cosets of  $C$  (which are of the form  $\underline{z} + C$  for some  $\underline{z} \in \mathbf{Z}_2^n$ ) form a *partition* of  $\mathbf{Z}_2^n$ . Further,  $\mathbf{Z}_2^n$  is the set of all *possible receivable* words  $\underline{r}$ .

**Form** the S.D.T. as follows: (i) As the *first row*, take the subgroup of code words  $C$  in any order, but **beginning** with  $\underline{0}$ . (ii) Take *subsequent* rows as the cosets of  $C$  in  $\mathbf{Z}_2^n$ . (iii) Begin each row with the *element* (or one of the elements) belonging to the coset which have minimum weight, then add this element to the corresponding **elements** of the first row ( $C$ ) to generate the coset. (iv) Decode received word  $\underline{r}$  by the code word at the *top* of the column.

**Example A:**  $m = 2, n = 5; E = ({}^1_0 \ 0_1 \ 1_0 \ 0_1 \ 1_1)$ . In the table shown on the right, the *first* row shows the possible message words while the *second* row shows the Code Words  $C$ . A value marked by an **asterisk** indicates “it is also of weight 2, an alternative leader”. In the table, we begin each coset row with a “**coset leader**” of minimum weight for that coset. Hence, start with all possible coset leaders of weight 1 such as 00001. Then, look at possible coset leaders of weight two. (Note: the *elements* of  $C$  (apart from  $\underline{0}$ ) are all of *weights 3 or 4*). Try 00110 (00011 has *already* occurred).

	00	01	10	11
00000	01011	10101	11110	
00001	01010	10100	11111	
00010	01001	10111	11101	
00100	01111	10001	11010	
01000	00011	11101	10110	
10000	11011	00101	01110	
00110	01101	10011	11000*	
01100	00111	11001	10010*	

The table *should* have  $2^n/2^m = 2^5/2^2 = 2^{n-m} = 2^3 = 8$  rows, each with  $2^m = 4$  elements. Then, for *example*,  $\underline{r} = (01101)$  is not a code word. Look in the **rest** of the table. Decode by the code word at the head of the column, i.e.  $\underline{r} = (01101) \rightarrow (01011) \rightarrow 01$ . Note that the *minimum distance* is the minimum weight of the non-zero code words. (For this code, it is 3, so it **detects** all errors of weights 1 and 2 and **corrects** all errors of weight 1).

28th March 2000

**Theorem:** The S.D.T. as just constructed decodes each *received* word  $\underline{r}$  to a nearest code word (minimum distance) as required. **Proof:** We prove that if  $\underline{r}_i$  is any received word; if  $\underline{c}_i$  is the code word at the *head* of the column containing  $\underline{r}_i$ ; and if  $\underline{c}_j$  is any **other** code word, then  $d(\underline{r}_i, \underline{c}_i) \leq d(\underline{r}_i, \underline{c}_j)$ .

Let  $\underline{e}$  be the “*coset leader*” for the row **containing**  $\underline{r}_i$ , and let  $\underline{r}_j$  be the entry in row ‘ $\underline{e}$ ’ and **under** code word  $\underline{c}_j$ . Then, by *definition*,  $\underline{r}_i = \underline{e} + \underline{c}_i$ ;  $\underline{r}_j = \underline{e} + \underline{c}_j$ ;  $d(\underline{r}_i, \underline{c}_i) = w(\underline{r}_i - \underline{c}_i) = w(\underline{e})$ ; and  $d(\underline{r}_i, \underline{c}_j) = w(\underline{r}_i - \underline{c}_j) = w(\underline{e} + \underline{c}_i - \underline{c}_j) = w(\underline{e} + \underline{c}_k)$ , where  $\underline{c}_i - \underline{c}_j = \underline{c}_k$  is **another** code word since  $C$  is a *subgroup*. By construction,  $\underline{e} + \underline{c}_k$  is in the  $\underline{e}$  row *under* code word  $\underline{c}_k$ . Since we chose  $\underline{e}$  to have **minimum** weight for this row, it follows that  $w(\underline{e}) \leq w(\underline{e} + \underline{c}_k)$ .

29th March 2000

## Parity Check Matrices

**Definition:** Given the  $m \times n$  *encoding matrix*  $E$ , we say that an  $n \times (n-m)$  matrix  $H$  is a parity check matrix for  $E$  iff  $\underline{r}H = 0 \Leftrightarrow \underline{r} \in C$  for all **received** words  $\underline{r} \in \mathbf{Z}_2^n$ . ( $C$  is the *subgroup* of code words). Notes: (1) Since the rows of  $E$  are *themselves* code words,  $\mathbf{E}H = \mathbf{0}$ . (2) If  $E$  is written in *standard form*:  $E = (I_m, P)$ , then  $H = \begin{pmatrix} P \\ I_{n-m} \end{pmatrix}$  is a *parity check matrix* for  $E$ .

**Definition:** If  $\underline{r} \in \mathbf{Z}_2^n$ , then we call  $\underline{r}H$  the *syndrome* of  $\underline{r}$  (for fixed  $H$ ). Note: since  $H$  is an  $n \times (n-m)$  matrix,  $\underline{r}H \in \mathbf{Z}_2^{(n-m)}$ . **Theorem:** Two *words* in  $\mathbf{Z}_2^n$  have the same *syndrome* iff they are in the same coset of  $C$  in  $\mathbf{Z}_2^n$  (and so in the same row of the S.D.T.). **Proof:**  $\underline{r}_1H = \underline{r}_2H \Leftrightarrow (\underline{r}_1 - \underline{r}_2)H = 0 \Leftrightarrow (\underline{r}_1 - \underline{r}_2) \in C \Leftrightarrow \underline{r}_1 + C = \underline{r}_2 + C$ .

**Note:** (i) In the S.D.T., any received word  $\underline{r}$  has the *same syndrome* as the “*coset leader*” at the beginning of the row. (ii) The number of **distinct** syndromes is the number of cosets  $= 2^{n-m} = |\mathbf{Z}_2^{(n-m)}|$ . Hence the *syndromes* constitute the whole of  $\mathbf{Z}_2^{(n-m)}$ . (This gives us a useful *check* on the syndrome).

**Example A:**  $E = ({}^1_0 \ 0_1 \ 1_0 \ 0_1 \ 1_1)$  ( $(\mathbf{I} \mid \mathbf{P})$ ,  $2 \times 5$ ). The *parity check matrix* for E is H, as shown on the right. Note that the first **two** rows is P and that the last **3** rows is I (a  $5 \times 3$  matrix). If  $\underline{r} = (01101)$ , then we can *recognise* that this belongs to the coset with leader (00110) from the fact that  $\underline{r}H = (01101)(H) = (110)$ . (**Note:** the (01101) picks out the *rows* for each *column*). And  $(00110)(H) = (110)$  (i.e. we have the same syndrome).

$$H = \begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

## New Decoding Procedure Using Syndromes

We can now **avoid** constructing the whole S.D.T. as follows: (a) List the message words  $\underline{a}$  and the code words  $\underline{c}$ , as *before*. (b) Calculate a Parity Check Matrix H for E. (c) Calculate the coset leaders  $\underline{e}$  (see below for the methods for *choosing* the leaders). (d) Calculate the syndromes of the coset leaders,  $\underline{e}H$ .

**Decoding.** For a received word  $\underline{r}$  (*not* a code word or there is **no** problem), (i) Calculate the syndrome  $\underline{r}H$ ; (ii) Identify the coset *leader*  $\underline{e}$  with the **same** syndrome, i.e.  $\underline{r}H = \underline{e}H$  — then  $\underline{e}$  is the coset *leader* for  $\underline{r}$ , and  $\underline{r} = \underline{e} + \underline{c}$  for some *code word*  $\underline{c} \in C$ , i.e.  $\underline{e}$  is the assumed *error* in  $\underline{r}$ ; (iii) Calculate  $\underline{c} = \underline{r} - \underline{e} = \underline{r} + \underline{e}$ . This  $\underline{c}$  would have been the **code word** at the top of the  $\underline{r}$  column in the S.D.T. (iv) *Decode*  $\underline{c} \rightarrow \underline{a}$ .

**Example A:** Let E and H be as before. The *first* column in the table shows the message words  $\underline{a}$ . The *second* column shows the code words  $\underline{c}$ . The *third* column shows the coset leaders  $\underline{e}$ , while the *fourth* column shows the syndromes  $\underline{e}H$ . **Note:** Syndromes are the **whole** of  $\mathbf{Z}_2^3$ . Example of *Decoding*:  $\underline{r} = (11101)$ ;  $\underline{r}H = (011)$ . The coset leader for  $\underline{r}$  is  $\underline{e} = (01000)$ .  $\underline{c} = \underline{r} - \underline{e} = \underline{r} + \underline{e} = (10101)$ , so  $\underline{a} = (10)$ .

00	00000	00000	000
01	01011	00001	001
10	10101	00010	010
11	11110	00100	100
		01000	011
		10000	101
		00110	110
		01100	111

## Hints for Choosing Coset Leaders

(i) If a coset leader produces the *previous syndrome*, then it must be **dropped** since this indicates that the coset has already occurred. (ii) Choose coset leaders, starting with those of weight 1, and try to keep the weight as **low** as possible. (iii) Near the end, choose coset leaders which give syndromes to complete  $\mathbf{Z}_2^{(n-m)}$ .

**Q:** Find a *parity check matrix* H, and give a table of coset leaders and syndromes. Use it to decode the received words  $\underline{r} = (01111)$  and  $\underline{r} = (00111)$ . **A:** We have  $E = ({}^1_0 \ 0_1 \ 1_0 \ 1_0 \ 1_1)$ , and so H is as shown on the **left**. The table on the right shows coset leaders  $\underline{e}$  in the *first* column and syndromes  $\underline{e}H$  in the *second*. For  $\underline{r} = (01111)$ ,  $\underline{r}H = (100)$ . So the coset **leader** for  $\underline{r}$  is  $\underline{e} = (00100)$ . Now  $\underline{c} = \underline{r} + \underline{e} = (00100) + (01111) = (01011)$ ; so  $\underline{a} = (01)$  by referencing the *previous* table. **Similarly**, if  $\underline{r} = (00111)$ ;  $\underline{r}H = (111)$ ;  $\underline{e} = (01100)$ ;  $\underline{c} = \underline{r} + \underline{e} = (01011)$ ; and  $\underline{a} = (01)$ .

00000	000
00001	001
00010	010
00100	100
01000	011
10000	110
00110	110 (No!)
01100	111
11000	101

a	c	wt.
000	00000000	0
001	0011101	4
010	0101011	4
011	0110110	4
100	1000111	4
101	1011010	4
110	1101100	4
111	1110001	4

**Example B:**  $m = 3$ ,  $n = 7$ , so  $n - m = 4$ . Here,  $E$  and  $H$  are as shown. Note that we can use the fact that  $E$  and  $H$  contain  $I$  to *simplify* calculation. The first table shown on the left shows the message words  $\underline{a}$  in the first column; the code words  $\underline{c}$  in the second column; and the *weights* in the third column. (The weights of the code words).

$$E = \begin{pmatrix} 1000111 \\ 0101011 \\ 0011101 \end{pmatrix} \quad H = \begin{pmatrix} 0111 \\ 1011 \\ 1101 \\ 1000 \\ 0100 \\ 0010 \\ 0001 \end{pmatrix}$$

In the **second** table on the right, we have the *coset leaders* in the first column; then the *weights*; then the *syndromes*; and finally the *binary representation* of the syndromes in  $\mathbf{Z}_2^4$ . **Note** that the \* means that at this point, we have exhausted the distinct cosets (syndromes) generated by weight 2 coset leaders. For example, the syndrome of 1000001 is 0110, so 1000001 occurs in the coset with leader 0000110. Example of **decoding**:  $\underline{r} = 1010111$ ;  $\underline{r}H = 1101$ ;  $\underline{e} = 0010000$ ;  $\underline{c} = \underline{r} + \underline{e} = 1000111$ ; so  $\underline{a} = 100$ .

coset lead	wt.	syndrome	
0000000	0	0000	0
0000001	1	0001	1
0000010	1	0010	2
0000100	1	0100	4
0001000	1	1000	8
0010000	1	1101	13
0100000	1	1011	11
1000000	1	0111	7
0000011	2	0011	3
0000110	2	0110	6
0001100	2	1100	12
0011000	2	0101	5
1010000	2	1010	10
0010100	2	1001	9
1001000	2	1111	15
0001110	3	1110	14

### Assignment 4: Set 29/3; In 5/4; Back 5/4

**Q:** Let  $p = 3$ ,  $q = 41$ ,  $n = pq = 123$ ,  $\phi(n) = 80$  and  $e = 67$  be an *RSA public key coding system*. Find the value of  $d$  and **decipher** the message 38, 05. **A:**  $d$  is an *integer* such that  $ed \equiv 1 \pmod{\phi(n)}$ , i.e.  $67d \equiv 1 \pmod{80}$ . We need to solve  $67d \equiv 1 \pmod{80}$  for  $d$ . Let us first *find*  $\gcd(67, 80)$ :  $\begin{pmatrix} 1 & 0 & 80 & 67 \\ 0 & 1 & 13 & 67 \end{pmatrix} \xrightarrow{R_1 - R_2} \begin{pmatrix} 1 & -1 & 67 & 1 \\ 0 & 1 & 13 & 67 \end{pmatrix} \xrightarrow{R_2 - 5R_1} \begin{pmatrix} 1 & -1 & 67 & 1 \\ 0 & 1 & 6 & 12 \end{pmatrix} \xrightarrow{R_1 + R_2} \begin{pmatrix} 1 & 0 & 73 & 13 \\ 0 & 1 & 6 & 12 \end{pmatrix} \xrightarrow{R_1 - 6R_2} \begin{pmatrix} 1 & 0 & 37 & 1 \\ 0 & 1 & 6 & 12 \end{pmatrix} \xrightarrow{R_2 - 2R_1} \begin{pmatrix} 1 & 0 & 37 & 1 \\ 0 & 1 & -6 & 10 \end{pmatrix}$ . So  $\gcd(67, 80) = 1 = 31 \times 80 - 37 \times 67$ . Therefore, the *inverse* of 67 is -37:  $67^{-1} \equiv -37 \pmod{80} \equiv 43 \pmod{80}$ . So  $\underline{d} = 43$ . Check:  $43 \times 67 = 2881 = 1 + (36 \times 80)$ . Now, we need to *decipher* the message 38, 05. To do this, we calculate  $38^{43} \pmod{123}$  and  $5^{43} \pmod{123}$ .

As  $43 = 32 + 8 + 2 + 1$ , we can *calculate*  $38^{43} \pmod{123}$  using the **powers** of 2:  $38^2 = 1444 \equiv 91 \pmod{123}$ ;  $38^4 \equiv 91^2 \equiv 8281 \equiv 40 \pmod{123}$ ;  $38^8 \equiv 40^2 \equiv 1600 \equiv 1 \pmod{123}$ ;  $38^{16} \equiv 1^2 \equiv 1 \pmod{123}$ ;  $38^{32} \equiv 1^2 \equiv 1 \pmod{123}$ ; so  $38^{43} = 1 \times 1 \times 91 \times 38 \equiv 3458 \equiv 14 \pmod{123}$ . Similarly,  $5^{43} \pmod{123} \equiv 2 \pmod{123}$ . So the *deciphered* message is 14, 02 — or NB.

**Q:** Let  $n = 123$  and  $e = 23$  be part of an *RSA public key coding system*. Encipher “BANGOR” using the usual scheme (A → 01, etc.). By **decomposing**  $n$  into its primes, find the value of  $d$ . Decipher the coded *message* 04, 50, 93. **A:** Bangor → 02, 01, 14, 07, 15, 18. To *encipher*, we must calculate  $r^{23} \pmod{133}$ .

As  $23 = 16 + 4 + 2 + 1$ , we can calculate  $2^{23} \pmod{133}$  using the *powers of 2*. So for B = 02,  $2^2 \equiv 4 \pmod{133}$ ;  $2^4 \equiv 16 \pmod{133}$ ;  $2^8 \equiv 123 \pmod{133}$ ;  $2^{16} \equiv 100 \pmod{133}$ ; so  $2^{23} \equiv 100 \times 16 \times 4 \times 2 \equiv 4 \times 4 \times 2 \equiv 32 \pmod{133}$ . Similarly, A:  $1^{23} \equiv 1 \pmod{133}$ ; N:  $14^{23} \equiv 105 \pmod{133}$ ; G:  $7^{23} \equiv 49 \pmod{133}$ ; O:  $15^{23} \equiv 78 \pmod{133}$ ; R:  $18^{23} \equiv 37 \pmod{133}$ . Therefore, when encoded, the **message** is 32, 1, 105, 49, 78, 37.

Now  $n = 133 = 7 \times 19$ , so  $\phi(n) = \phi(7 \times 19) = 6 \times 18 = 108$ . To find  $d$ , we must solve  $23d \equiv 1 \pmod{108}$ . Start by finding  $\gcd(23, 108)$  using the matrix method:  $\gcd(23, 108) = 1 = -10 \times 108 + 47 \times 23$ . Therefore, the **inverse** of 23 is 47, or  $23^{-1} \equiv 47 \pmod{108}$ ; so  $d = 47$ . **Check:**  $47 \times 23 = 1081 = 1 + (10 \times 108)$ .

Now we need to *decipher* the message 04, 50, 93. To do this, we need to *calculate* the following:  $4^{47} \pmod{133}$ ;  $50^{47} \pmod{133}$ ; and  $93^{47} \pmod{133}$ . Again, we *split 47 up* as  $47 = 32 + 8 + 4 + 2 + 1$ , and calculate the **powers** of 2. Finding that  $4^{47} \equiv 16 \pmod{133}$ ;  $50^{47} \equiv 8 \pmod{133}$ ; and  $93^{47} \equiv 4 \pmod{133}$ , the *deciphered* message is 16, 8, 4 — or PHD.

Q: A matrix code has encoding matrix as **shown**. Write down a parity check matrix for this code. Construct a table of *message* words and *code* words. Construct a table of coset leaders and syndromes. Decode the message 101101, 110110, 110101, 110011, 101010, 011100.  $E = \begin{pmatrix} 1 & 0 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 \end{pmatrix}$

Message Words <u>a</u>	Code Words <u>c</u>	Weight (of <u>c</u> )
000	000000	0
001	001011	3
010	010101	3
100	100110	3
110	110011	4
101	101101	4
011	011110	4
111	111000	3

A: A parity check matrix for  $E$  is given by  $H$  as shown, where the *first three rows* consist of  $P$  and the *last three rows* are  $I_3$ . On the left is a table for the possible message words a (which are of *length 3*) and their associated **code** words c, given by  $\underline{c} = \underline{a}E$ . Note that *calculation* of  $\underline{c} = \underline{a}E$  is simplified by knowing that in a, each element which is 1 simply adds the corresponding **row** in  $E$  to c.  $H = \begin{pmatrix} 1 & 1 & 0 \\ 1 & 0 & 1 \\ 0 & 1 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$

The table on the *right* shows the coset leaders and syndromes. The last column shows the syndrome as a **binary** representation of an integer. Note that in the last row, after exhausting all coset leaders of weights 0 and 1, we get the *remaining* syndrome (1 1 1) by noticing that we can get the missing syndrome by adding **two** rows of  $H$  — I have chosen the third and fourth rows to accomplish this. To decode,

<u>r</u>	<u>rH</u>	<u>e</u>	<u>c=r+e</u>	<u>a</u>
101101	000	000000	101101	101
110110	101	010000	100110	100
110101	110	100000	010101	010
110011	000	000000	110011	110
101010	111	001100	100110	100
011100	010	000010	011110	011

I will use a table as shown on the *left*. Note that because the minimum weight of a non-zero code word is 3, we can **detect** all errors of weights 1 and 2; and **correct** all errors of weight 1. Therefore, in the table on the left, all decoded message words a are correct except for the *fifth* row, as because we have an error vector of weight 2, we can only **detect** the error, and the message word a given here is **not** unique.

Coset Leader <u>e</u>	Syndrome <u>eH</u>	$Z_2^3$
000000	000	0
000001	001	1
000010	010	2
000100	100	4
001000	011	3
010000	101	5
100000	110	6
001100	111	7*

How is the table *constructed*? Each message we wish to decode is placed in the **1st** column. Post multiply by  $H$  and place in the *second* column. Look for the result amongst the syndromes, and write down the corresponding coset leader in the **third** column. To produce a code word, add the vectors r and e, and place the result in the *fourth* column. Then look for this code word in the code words **table**, and report back the message word and place it in *the* last column as the decoded result a.

## Probability for S.D.T.

If the *received* word  $\underline{r}$  is not a code word, then we decode  $\underline{r}$  as the **code** word  $\underline{c}$  at the head of the column *containing*  $\underline{r}$  in the S.D.T., where  $\underline{r} = \underline{c} + \underline{e}$ , and  $\underline{e}$  is the **coset leader** at the beginning of the row. Hence iff the *error* vector of  $\underline{r}$  is indeed a *coset leader*, we therefore decode correctly.

Recall that the probability of **producing** error vectors of weight  $w$  is  $\binom{n}{w} p^{n-w} q^w$ , with the probability of producing *error* vectors of weight  $w$  with errors in **prescribed** order being  $p^{n-w} q^w$ . Hence the probability of *correctly decoding* something is  $\sum \alpha_i p^{n-i} q^i$ , where  $\alpha_i$  is the number of *coset leaders* of **weight**  $i$ . (This does not usually cover **all**  $\binom{n}{i}$  possibilities).

**The probability of undetected errors.** The fact that there has been an *error* will go undetected if  $\underline{r}$  is a code word *different* from the original. This occurs iff the error  $(\underline{r} - \underline{c}) \in C$ . Hence the undetected errors are **equal** to the *non-zero* code words. The probability of an undetected error is  $\sum \beta_i p^{n-i} q^i$ , where  $\beta_i$  is the number of *code* words of weight  $i$  ( $i \geq 1$ ).

**In Example A,** the number of *coset leaders* of weight 0 is 1; weight 1 = 5; and weight 2 = 2. So the *probability of correct decoding* is  $1 \cdot p^5 q^0 + 5 p^4 q^1 + 2 p^3 q^2 = p^5 + 5 p^4 q + 2 p^3 q^2$ . The number of *code words* of weight 3 is 2; weight 4 = 1. Thus the probability of an undetected error is  $2 p^2 q^3 + p q^4$ . **In Example B,** the probability of *correct decoding* is  $p^7 + 7 p^6 q + 7 p^5 q^2 + p^4 q^3$ ; and the probability of an *undetected error* is  $7 p^3 q^4$ .

Q: (Continuation): If the probability of *correct reception* of a single digit is  $p = 0.9$ , find the probability of correct decoding of a **received** word, and the probability of an undetected **error**. The number of coset leaders of weight 0 is 1; weight 1 = 5; weight 2 = 2. Thus the probability of *correct decoding* is  $p^5 + 5 p^4 q + 2 p^3 q^2 = 0.93312$ . The number of code words of weight 3 is 2; weight 4 = 1. Thus the probability of an *undetected error* is  $2 p^2 q^3 + p q^4 = 2 \times 0.9^2 \times 0.1^3 + 0.9 \times 0.1^4 = 0.00171$ .

## Hamming Codes

Let  $r \geq 2$  and consider *all possible binary representations* of integers as elements of  $\mathbf{Z}_2^r$ . For example,  $\underline{r} = 2$ :  $\mathbf{Z}_2^2$  is  $00 = 0$ ;  $01 = 1$ ;  $10 = 2$ ; and  $11 = 3 = 2^2 - 1$ . For  $\underline{r} = 3$ , we get all the integers up to  $2^3 - 1$ , etc. Form a matrix  $H$  with the **non-zero** binary representations as rows.  $H$  will be a  $(2^r - 1) \times r$  matrix. For  $\underline{r} = 2$ ,  $H = \begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 1 \end{pmatrix}$ , a  $(2^2 - 1) \times 2$  matrix. In *standard* form,  $H = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ .

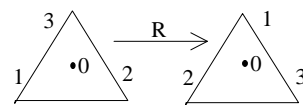
The **code** for which  $H$  is a *parity check matrix* is called a Hamming code. **Notes:** (1) A Hamming code has *minimum* distance 3, and so always corrects all single errors. (2) A Hamming code is “perfect” in the sense that each word of  $\mathbf{Z}_2^n$  ( $n = 2^r - 1$ ) is either a *code word* or is at a distance 1 from a unique code word.

# Chapter 6: Further Group Theory

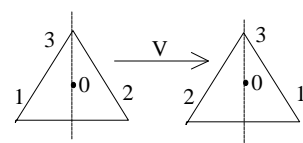
## Symmetry Groups

The *symmetries* of regular geometrical figures form groups.

**Example 1:** Equilateral Triangle. Let R be a rotation about O through  $2\pi/3$ , which replaces 1 by 2; 2 by 3; and 3 by 1. As a permutation of the *vertices*, R is equivalent to  $(\begin{smallmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{smallmatrix}) = (1\ 2\ 3)$ . Then  $R^2 =$  the rotation through  $4\pi/3$ , equivalent to  $(1\ 3\ 2)$ ; and  $R^3 = I$ , so R will not *generate* any further symmetries.



Let V be the **reflection** in the line O3. As a permutation of vertices, V is equivalent to  $(\begin{smallmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{smallmatrix})$  or  $(1\ 2)$ .  $V^2 = I$ , so we cannot *generate* any further symmetries using V alone. There are two other reflections (in O1 and O2), and we can express these in **terms** of R and V. **VR** (R first) gives

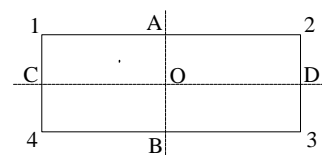


the diagram on the *left*, resulting in a reflection in O1. Equivalently in terms of *permutations*,  $(1\ 2)(1\ 2\ 3) = (\begin{smallmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{smallmatrix}) = (2\ 3)$ . Also, **VR<sup>2</sup>** gives the *reflection* in the line O2, or equivalently the **permutation**  $(1\ 3)$ .

The *other possible combinations* of V & R are RV and R<sup>2</sup>V. However, RV gives  $(1\ 2\ 3)(1\ 2) = (\begin{smallmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{smallmatrix}) = (1\ 3) = VR^2 = VR^{-1}$ ; and *similarly*  $R^2V = VR$ . Therefore, the group of symmetries is  $\{I, R, R^2, V, VR, VR^2\}$ , which is **isomorphic** to  $S_3$  (the same “*as a group*”), with  $R^3 = I = V^2$ , and  $RV = VR^2 = VR^{-1}$ .

**Example 2:** In general, a *regular n-sided polygon* gives all symmetries as combinations of a rotation R through  $2\pi/n$  and a reflection V. The *group* is  $\{I, R, R^2, \dots, R^{n-1}, V, VR, VR^2, \dots, VR^{n-1}\}$ ; it is of order 2n; and it is called the *Dihedral Group*,  $D_n$ , where  $R^n = I = V^2$ , and  $RV = VR^{n-1} = VR^{-1}$ . **Example 3:** Regular *Tetrahedron* (3 dimensions) The symmetries give all possible permutations of the vertices 1, 2, 3 and 4, i.e. the group  $S_4$ .

**Example 4:** Rectangle (not a square). Let R be the *rotation* through  $\pi$ ,  $R = (\begin{smallmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 1 & 2 \end{smallmatrix}) = (1\ 3)(2\ 4)$ . It follows that  $R^2 = I$ . Now let V be the reflection in the *line* AOB,  $V = (\begin{smallmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{smallmatrix}) = (1\ 2)(3\ 4)$ . It follows that  $V^2 = I$ . Now  $RV = (\begin{smallmatrix} 1 & 2 & 3 & 4 \\ 2 & 4 & 1 & 3 \end{smallmatrix}) = (1\ 4)(3\ 2) =$  the reflection COD. Finally,  $VR = RV$ . Thus the *group* is  $\{I, R, V, VR\}$ , where  $R^2 = V^2 = I$ , and  $VR = RV$ . This is **Kleins 4-group**, a *subgroup* of  $S_4$ .



## Group Presentation

**Definition:** A group presentation consists of a *set of generators*, and *relations* between them. These define a group consisting of all possible **distinct** products of the generators. For example, examples 1, 2 and 4 above — with R and V as generators; and relations as **given**. The cyclic groups  $C_n$  is generated by “a”, where  $a^n = 1$ , i.e.  $C_n = \{a: a^n = 1\} = \{1, a, a^2, \dots, a^{n-1}\}$ .

## Direct Products of Groups

**Definition:** The direct product of groups  $G$  and  $H$  is the set of ordered pairs  $G \times H = \{(g,h): g \in G, h \in H\}$  with multiplication defined by  $(g_1, h_1)(g_2, h_2) = (g_1 g_2, h_1 h_2)$ , where the multiplication of the  $g_i$  and the  $h_i$  take place in  $G$  and  $H$  respectively. With this definition,  $G \times H$  is a group with identity  $(I_G, I_H)$  ( $I_G$  is the identity of  $G$ ;  $I_H$  is the identity of  $H$ ), and the inverse of  $(g,h)$  in  $G \times H$  is  $(g^{-1}, h^{-1})$ .

**Example:**  $G = C_2 \times C_2$ . To avoid confusion, take  $C_2 = \{1, a\}$ ,  $a^2 = 1$ ; and  $C_2 = \{1, b\}$ ,  $b^2 = 1$ . Then  $G = \{(1,1), (1,b), (a,1), (a,b)\}$ , with Cayley table as shown on the right. Note that  $(1,b)^2 = (1,1) = (a,1)^2$ ; and  $(1,b)(a,1) = (a,b) = (a,1)(1,b)$ . The correspondence  $I \Leftrightarrow (1,1)$ ;  $R \Leftrightarrow (1,b)$ ; and  $V \Leftrightarrow (a,1)$  shows that  $C_2 \times C_2$  is isomorphic to Klein's 4 group.

	(1,1)	(1,b)	(a,1)	(a,b)
(1,1)	(1,1)	(1,b)	(a,1)	(a,b)
(1,b)	(1,b)	(1,1)	(a,b)	(a,1)
(a,1)	(a,1)	(a,b)	(1,1)	(1,b)
(a,b)	(a,b)	(a,1)	(1,b)	(1,1)

**Example:**  $C_2 \times C_3 \simeq C_6$  (Isomorphic). Take  $C_2 = \{1, a\}$  ( $a^2 = 1$ ) and  $C_3 = \{1, b, b^2\}$  ( $b^3 = 1$ ). Then  $C_2 \times C_3 = \{(1,1), (1,b), (a,1), (a,b), (a,b^2), (1,b^2)\}$ . Further,  $(a,b)^2 = (a^2, b^2) = (1, b^2)$ ;  $(a,b)^3 = (a,1)$ ;  $(a,b)^4 = (1,b)$ ;  $(a,b)^5 = (a,b^2)$ ; and  $(a,b)^6 = (1,1)$ . Hence  $C_2 \times C_3$  is cyclic of order 6, with generator  $(a,b)$ .

## Normal Subgroups

(1) A subgroup  $S$  of a group  $G$  is called **normal** iff  $g^{-1}sg \in S$  for all  $g \in G$  and for all  $s \in S$ . (2) A subgroup  $S$  is normal iff  $g^{-1}Sg = S$  for all  $g \in G$ . (Recall that  $g^{-1}Sg = \{g^{-1}sg: g \in G, s \in S\}$ ). These are *equivalent*. **Proof:** Clearly (2)  $\Rightarrow$  (1). Now assume (1). Fix  $g \in G$ . Then  $g^{-1}Sg \subseteq S$ . We must show that  $S \subseteq g^{-1}Sg$ .

Let  $s \in S$ , so that  $s = g^{-1}(gsg^{-1})g = g^{-1}(g^{-1}sg)^{-1}g$ . By assumption,  $g^{-1}sg \in S$ ; and we know that  $S$  is a subgroup, so that  $(g^{-1}sg)^{-1} \in S$ , i.e.  $S$  is of the form  $g^{-1}s^*g \in g^{-1}Sg$ , as required. **Natural Definition:** Let  $f: G \rightarrow H$  be a group homomorphism, so that  $(f(g_1 g_2)) = f(g_1) \cdot f(g_2)$ . Then the "Kernel" of  $f$  is  $\text{Ker } f = \{g \in G, f(g) = I_H\}$ . Note:  $\text{Ker } f$  is a **normal** subgroup of  $G$ .

**Proof:** (i) Let  $a, b \in \text{Ker } f \subseteq G$ , so that  $f(a) = f(b) = I_H$ . Further,  $f(ab^{-1}) = f(a)f(b^{-1}) = f(a)(f(b))^{-1} = I_H \cdot I_H = I_H$ , i.e.  $ab^{-1} \in \text{Ker } f$ ;  $\text{Ker } f$  is a subgroup. (ii) Let  $g \in G$  and let  $s \in \text{Ker } f$ , so that  $f(g^{-1}sg) = f(g^{-1})f(s)f(g) = (f(g))^{-1}I_H f(g) = I_H$ , i.e.  $g^{-1}sg \in \text{Ker } f$ , as required.

**Example:** Consider  $\phi: C_4 = \{1, a, a^2, a^3\} \rightarrow C_2 = \{1, b\}$ , with  $a^4 = 1$  and  $b^2 = 1$ . Define the function by  $\phi: 1$  and  $a^2$  go to 1;  $a$  and  $a^3$  go to  $b$ . This is a **group homomorphism** with Kernel =  $\{1, a^2\}$ , a normal subgroup of  $C_4$ . (In fact,  $\text{Ker } \phi = \{1, a^2\} \simeq C_2$ , with generator  $a^2$ ). It is clear from the definition that all subgroups of an **Abelian** group are normal, since  $g^{-1}sg = g^{-1}gs = s$ .

## Quotient Groups (Factor Groups)

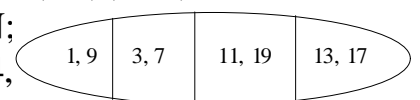
Recall that if  $N$  is a *normal* subgroup of  $G$ , then the **left** cosets  $gN$  form a partition of  $G$ . Now define *multiplication* of cosets by  $(aN)(bN) = \{g = g_1g_2 : g_1 \in aN, g_2 \in bN\}$ , and then we show that  $(aN)(bN) = (ab)N$  for all  $a, b \in G$ . In particular, the *multiplication* of cosets gives another coset of  $N$ .

**Proof:** (i)  $(aN)(bN) \subseteq (ab)N$ . Let  $g \in (aN)(bN)$ , then  $g = (an_1)(bn_2)$  for some  $n_1, n_2 \in N$ , i.e.  $g = a(bb^{-1})n_1bn_2 = (ab)(b^{-1}n_1b)n_2$ , where  $b^{-1}n_1b \in N$  since  $N$  is **normal**. Thus we can write this expression as  $(ab)n_3$  for some  $n_3 \in N$ , i.e.  $g \in (ab)N$ . (ii)  $(ab)N \subseteq (aN)(bN)$ . Let  $g \in (ab)N$ , then  $g = (ab)n$  for some  $n \in N$ . And  $g = abn(b^{-1}b) = (a(bnb^{-1}))(b.1)$ , where  $bnb^{-1} = (b^{-1}nb)^{-1} \in N$ , since  $N$  is a *normal* subgroup, and  $1 \in N$ , i.e.  $g \in (aN)(bN)$ .

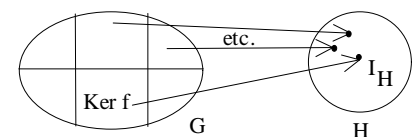
**Theorem:** The set of *left cosets* of  $N$  in  $G$ , denoted by  $G/N$ , form a group under coset multiplication. **Proof:** Closure. Already Proved. Associativity: Let  $aN, bN, cN \in G/N$ . Then  $((aN)(bN))(cN) = ((ab)N)(cN) = (ab)cN =$  (since  $G$  is *associative*)  $= a(bc)N = (aN)((bc)N) = (aN)((bN)(cN))$ . Identity:  $I_{G/N} = N = 1.N$ , since  $(1N)aN = (1a)N = aN = (a.1)N = (aN)(1N)$ . Inverse:  $(aN)^{-1} = (a^{-1}N)$ , since  $(aN)(a^{-1}N) = (aa^{-1})N = 1.N = N = (a^{-1}a)N = (a^{-1}N)(aN)$ .

**Definition:** We call  $G/N$  the *quotient* group of  $G$  by  $N$  (remember that  $N$  has to be a *normal* subgroup). **Example:**  $G = U(\mathbf{Z}_{20}^*) = \{1, 3, 7, 9, 11, 13, 17, 19\}$ , with *multiplication* mod 20. This is an Abelian group, so that all subgroups are normal. Further,  $9^2 \equiv 1 \pmod{20}$ , so  $N = \{1, 9\}$  is a *normal* subgroup of order 2 ( $\simeq C_2$ ).

The *left cosets* of  $N$  are:  $1.N = \{1, 9\} = 9.N$ ;  $3.N = \{3, 3.9 \equiv 7\} = 7.N$ ;  $11.N = \{11, 19\} = 19.N$ ; and  $13.N = \{13, 17\} = 17.N$ . Thus  $G/N$  can be represented as in the diagram, where, for example,  $\{3, 7\}\{11, 19\} = (3N)(11N) = (3.11 \equiv 13)N = \{13, 17\}$ . (or  $(7N)(19N) = 7.19 \equiv 13 = \{13, 17\}$ . In fact,  $(13N)^2 = (13.13)N = 9N$ ;  $(13N)^3 = (13.9)N = 17N$ ; and  $(13N)^4 = (13.17)N = 1N$ . So  $G/N$  is a *cyclic* group of order 4, **generated** by  $13N$ .



**Theorem:** Let  $f: G \rightarrow H$  be a group *homomorphism*, then  $f(x) = f(y)$  iff  $x$  and  $y$  belong to the same coset of  $G/\text{Ker } f$ . **Proof:** (i) Assume  $f(x) = f(y)$ , then  $f(x^{-1}y) = f(x^{-1})f(y) = (f(x))^{-1}f(y) = (f(y))^{-1}f(y) = I_H$ , i.e.  $x^{-1}y \in \text{Ker } f$ .



Then *both*  $x$  and  $y$  belong to the **coset**  $x\text{Ker } f$  (clearly  $x \in x\text{Ker } f$ ) since  $y = x(x^{-1}y) \in x\text{Ker } f$ . In fact,  $x\text{Ker } f = y\text{Ker } f$ . (ii) **Assume that**  $x$  and  $y \in x\text{Ker } f$ , i.e.  $y = xk$  for some  $k \in \text{Ker } f$  (where  $f(k) = 1$ ). **Then**  $f(y) = f(xk) = f(x)f(k) = f(x)$ .

## The First Isomorphism Theorem

If  $f: G \rightarrow H$  is a group *homomorphism*, then  $G/\text{Ker } f \simeq f(G)$ . **Proof:** ( $f(G)$  is a *subgroup* of  $H$ ;  $\text{Ker } f$  is a *normal subgroup* of  $G$ ): Define a *function*  $\theta: G/\text{Ker } f \rightarrow f(G)$ , by  $\theta(x\text{Ker } f) = f(x)$  for all *cosets*  $x\text{Ker } f \in G/\text{Ker } f$ . By the **previous** theorem, this is a well defined *injective* function on  $G/\text{Ker } f$ . By the definition of  $f(G)$ , it is **surjective**.

It remains to show that  $\theta$  is a *group homomorphism*:  $\theta((x\text{Ker } f)(y\text{Ker } f)) = \theta((xy)\text{Ker } f) =$  (by the *definition* of  $\theta$ )  $= f(xy) = f(x)f(y) = \theta(x\text{Ker } f)\theta(y\text{Ker } f)$ .

**Example:** Let  $\mathbf{Z}$  be the group of *integers* under addition, and let  $\mathbf{Z}_m = \{0, 1, \dots, m-1\}$  be the group of integers under *addition mod m*. Let  $f: \mathbf{Z} \rightarrow \mathbf{Z}_m$  be defined by reducing each  $n \in \mathbf{Z}$  to the unique *equivalent* in  $\mathbf{Z}_m$ . (By *modulo m* operations).  $\text{Ker } f = m\mathbf{Z}$ , and by the first *Isomorphism Theorem*,  $\mathbf{Z}/\text{Ker } f$ , i.e.  $\mathbf{Z}/m\mathbf{Z} \simeq \mathbf{Z}_m$ .

## Exam Paper: May 2000

### SECTION 1 (Compulsory)

- (1) (a) Find the multiplicative inverse of 169 modulo 391. **[3 marks]**
- (b) Show that the matrix  $\begin{pmatrix} 2 & 1 \\ 7 & 5 \end{pmatrix}$  is invertible modulo 26 and calculate its inverse. **[4 marks]**
- (c) Let  $\alpha = (147)(258)(369)(123456789)$  be an element of the permutation group  $S_9$ . Write  $\alpha$  as a product of disjoint cycles, and also as a product of transpositions. **[4 marks]**
- (d) Find the last two digits of  $43^{4443}$ . **[4 marks]**
- (e) Show that  $n^{67} \equiv n$  modulo 469 for all  $n \in \mathbf{Z}$ . **[5 marks]**

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

- (2) (a) Let  $*$  be a closed binary operation on a set  $S$ . Give the properties which need to be satisfied for  $S$  with  $*$  to form a group. **[3 marks]**
- (b) Define  $x*y = 2xy+x+y$  where  $x, y \in \mathbb{R}$  and let  $S = \mathbb{R} \setminus \{-1/2\}$ . Show that  $S$  with  $*$  forms a group. **[12 marks]**
- (3) (a) State Lagrange's Theorem and Euler's Theorem. **[2 marks]**
- (b) Prove Euler's Theorem using Lagrange's Theorem. **[7 marks]**
- (c) Find a generator for the multiplicative cyclic group  $\mathbf{Z}_{11}^* = \{1, 2, 3, \dots, 9, 10\}$ , and hence find all possible generators. **[6 marks]**
- (4) (a) Describe the main features of the R.S.A. public key coding system. **[4 marks]**
- (b) In an R.S.A. public key coding system the public key is  $n = 111$  and  $e = 65$ . Encode the message 07, 15. **[4 marks]**
- (c) By decomposing  $n$  into its prime factors decode the message 98, 29, 49, 18. **[7 marks]**

(5) A matrix code has the encoding matrix

$$E = \begin{bmatrix} 1 & 0 & 0 & 1 & 0 & 0 & 1 \\ 0 & 1 & 0 & 1 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 0 & 1 & 1 \end{bmatrix}$$

- (a) Write down a parity check matrix for this code. **[1 mark]**
- (b) Construct a table of message words and code words. **[3 marks]**
- (c) Construct a table of coset leaders and syndromes and use it to decode the message 1110100, 0101111, 1000100. **[8 marks]**
- (d) If  $p$  is the probability of correct reception of one digit, find in terms of  $p$  and  $q = 1-p$  the probability of correct decoding of one word. **[3 marks]**

(Questions done: 1, 2, 5)