MATH 433

Applied Algebra

Lecture 38:
Review for the final exam (continued).

Topics for the final exam: Part I

- Mathematical induction, strong induction
- Greatest common divisor, Euclidean algorithm
- Primes, factorisation, Unique Factorisation Theorem
- Congruence classes, modular arithmetic
- Inverse of a congruence class
- Linear congruences
- Chinese Remainder Theorem
- Order of a congruence class
- Fermat's Little Theorem, Euler's Theorem
- Euler's phi-function
- Public key encryption, the RSA system

Topics for the final exam: Part II

- Relations, properties of relations
- Finite state machines, automata

- Permutations
- Cycles, transpositions
- Cycle decomposition of a permutation
- Order of a permutation
- Sign of a permutation
- Symmetric and alternating groups

- Abstract groups (definition and examples)
- Semigroups
- Rings, zero-divisors
- Fields, characteristic of a field
- Vector spaces over a field

Topics for the final exam: Part III

- Order of an element in a group
- Subgroups
- Cyclic groups
- Cosets
- Lagrange's Theorem
- Isomorphism of groups

- The ISBN code
- Binary codes, error detection and error correction
- Linear codes, generator matrix
- Coset leaders, coset decoding table
- Parity-check matrix, syndromes

- Division of polynomials
- Greatest common divisor of polynomials
- Factorisation of polynomials

Problem. You receive a message that was encrypted using the RSA system with public key $(65, 29)$, where 65 is the base and 29 is the exponent. The encrypted message, in two blocks, is $3/2$. Find the private key and decrypt the message.

First we find $\phi(65)$. Prime factorisation: $65 = 5 \cdot 13$. Hence $\phi(65) = \phi(5)\phi(13) = (5-1)(13-1) = 48$.

The private key is $(65, \beta)$, where the exponent β is the inverse of 29 (the exponent from the public key) modulo $\phi(65) = 48$. To find β, we apply the Euclidean algorithm to 29 and 48:

$$\left(\begin{array}{cc|c} 1 & 0 & 29 \\ 0 & 1 & 48 \end{array}\right) \to \left(\begin{array}{cc|c} 1 & 0 & 29 \\ -1 & 1 & 19 \end{array}\right) \to \left(\begin{array}{cc|c} 2 & -1 & 10 \\ -1 & 1 & 19 \end{array}\right)$$
$$\to \left(\begin{array}{cc|c} 2 & -1 & 10 \\ -3 & 2 & 9 \end{array}\right) \to \left(\begin{array}{cc|c} 5 & -3 & 1 \\ -3 & 2 & 9 \end{array}\right).$$

From the first row: $5 \cdot 29 - 3 \cdot 48 = 1$, which implies that 5 is the inverse of 29 modulo 48.

Decrypted message: b_1/b_2, where $b_1 \equiv 3^5 \bmod 65$, $b_2 \equiv 2^5 \bmod 65$. We find that $b_1 = 48$, $b_2 = 32$.

Problem. Let f be a linear coding function defined by the generator matrix $\begin{pmatrix} 1 & 0 & 0 & 0 & 1 & 1 & 1 \\ 0 & 1 & 0 & 1 & 0 & 1 & 1 \\ 0 & 0 & 1 & 1 & 1 & 0 & 1 \end{pmatrix}$.

Suppose that a message encoded by f is received with errors as 1011101 1101100 0110111. Correct errors and decode the received message.

The 8 codewords are linear combinations of rows of the generator matrix:

$$\begin{matrix} 0000000 & 0011101 & 0101011 & 1000111 \\ 0110110 & 1011010 & 1101100 & 1110001 \end{matrix}$$

Minimal weight of nonzero codewords: 4. Hence the code detects 3 errors and corrects 1. Every received word is at distance ≤ 1 from a codeword. The corrected message is

0011101 1101100 0110110

The code is systematic, hence decoding consists of truncating the codewords to 3 digits: 001 110 011 (1 6 3).

Alternatively, we can correct the received message using coset leaders and syndromes. First we transform the generator matrix G into the parity-check matrix P:

$$\left(\begin{array}{ccc|cccc} 1 & 0 & 0 & 0 & 1 & 1 & 1 \\ 0 & 1 & 0 & 1 & 0 & 1 & 1 \\ 0 & 0 & 1 & 1 & 1 & 0 & 1 \end{array}\right) \to \left(\begin{array}{cccc} 0 & 1 & 1 & 1 \\ 1 & 0 & 1 & 1 \\ 1 & 1 & 0 & 1 \\ \hline 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{array}\right)$$

For any word $u \in \mathbf{B}^7$, its syndrome is the product uP.

Next we build a table of coset leaders and their syndromes. Clearly, the zero word is a coset leader. Since the code can correct 1 error, all words of weight 1 are coset leaders as well (their syndromes are rows of P). The other eight syndromes correspond to coset leaders of weight 2 or more.

Coset leaders	Syndromes
0000000	0000
1000000	0111
0100000	1011
0010000	1101
0001000	1000
0000100	0100
0000010	0010
0000001	0001
0000011	0011
0000101	0101
0001001	1001
0000110	0110
0001010	1010
0001100	1100
0001110	1110
1001000	1111

$$
(1\,0\,1\,1\,1\,0\,1)\begin{pmatrix}0 & 1 & 1 & 1\\ 1 & 0 & 1 & 1\\ 1 & 1 & 0 & 1\\ 1 & 0 & 0 & 0\\ 0 & 1 & 0 & 0\\ 0 & 0 & 1 & 0\\ 0 & 0 & 0 & 1\end{pmatrix} = (0\,1\,1\,1)
$$

$$
(1\,1\,0\,1\,1\,0\,0)\begin{pmatrix} 0 & 1 & 1 & 1 \\ 1 & 0 & 1 & 1 \\ 1 & 1 & 0 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} = (0\,0\,0\,0)
$$

$$(0\,1\,1\,0\,1\,1\,1)\begin{pmatrix}0 & 1 & 1 & 1\\ 1 & 0 & 1 & 1\\ 1 & 1 & 0 & 1\\ 1 & 0 & 0 & 0\\ 0 & 1 & 0 & 0\\ 0 & 0 & 1 & 0\\ 0 & 0 & 0 & 1\end{pmatrix} = (0\,0\,0\,1)$$

Now we can start the error correction. For each received word u we calculate the syndrome uP and find a coset leader $\tilde{u}$ with the matching syndrome. Then the corrected word is $u - \tilde{u}$.

Received	Syndrome	Coset leader	Corrected
1011101	0111	1000000	0011101
1101100	0000	0000000	1101100
0110111	0001	0000001	0110110

The code is systematic, hence decoding consists of truncating the codewords to 3 digits: 001 110 011.

Problem. Find two non-Abelian groups of order 24 that are not isomorphic to each other.

It is known that groups of order 24 form 15 isomorphism classes. Three of them are Abelian groups, represented by $\mathbb{Z}_3 \times \mathbb{Z}_8$, $\mathbb{Z}_3 \times \mathbb{Z}_4 \times \mathbb{Z}_2$, and $\mathbb{Z}_3 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$.

The other 12 classes are non-Abelian groups. Representatives for some of them are: $S(4)$, $A(4) \times \mathbb{Z}_2$, $S(3) \times \mathbb{Z}_4$, $S(3) \times \mathbb{Z}_2 \times \mathbb{Z}_2$, $D(12)$, $D(4) \times \mathbb{Z}_3$, and $SL(2, \mathbb{Z}_3)$.

Center of a group

Definition. Given a group G, an element $c \in G$ is called **central** if it commutes with any element of the group: $cg = gc$ for all $g \in G$. The set of all central elements, denoted $C(G)$, is called the **center** of G.

$C(G)$ is a normal subgroup of G. If $f : G \to H$ is an isomorphism of groups, then $f(C(G)) = C(H)$ so that $C(G) \cong C(H)$. Hence $C(G) \not\cong C(H) \implies G \not\cong H$.

- If G is Abelian then $C(G) = G$.
- Center of $S(n)$ is trivial for $n \geq 3$.
- Center of $A(n)$ is trivial for $n \geq 4$.
- $C(D(2n)) = \{\text{identity map, rotation by } 180^\circ\}$.
- $C(D(2n+1)) = \{\text{identity map}\}$.
- Center of $GL(n, \mathbb{F})$ consists of scalar matrices αI, where $\alpha \in \mathbb{F}$, $\alpha \neq 0$.
- $C(G_1 \times G_2 \times \cdots \times G_k) = C(G_1) \times C(G_2) \times \cdots \times C(G_k)$.