MAT 3343, APPLIED ALGEBRA, FALL 2003

Answers to the Midterm

Problem 1. Let $m, n \in \mathbb{Z}$ and $m \geqslant 0$. Prove that $m|n$ iff $\gcd(m, n) = m$.

Answer: "$\Rightarrow$": Suppose $m|n$. But also $m|m$, so m is a common divisor of m, n. To show that it is a greatest common divisor, assume k is another common divisor. But then $k|m$, hence m is a greatest common divisor. Thus $m = \pm \gcd(m, n)$. Since $m \geqslant 0$, it follows that $m = \gcd(m, n)$.

"$\Leftarrow$": Suppose $\gcd(m, n) = m$. Then m is a common divisor of m, n, hence $m|n$.

Problem 2. How many solutions does the equation $x^2 = 9$ have in $\mathbb{Z}_{77}$? Find all solutions.

Answer: Since $77 = 7 \cdot 11$, and $7, 11$ are relatively prime, we know by the Chinese Remainder Theorem that $x^2 \equiv 9 (\operatorname{mod} 77)$ if and only if

$$\begin{array}{lll} (1) & x^2 \equiv 9 (\operatorname{mod} 7) & \text{and} \\ (2) & x^2 \equiv 9 (\operatorname{mod} 11). & \end{array}$$

Since 7 and 11 are prime, $\mathbb{Z}_7$ and $\mathbb{Z}_{11}$ are fields, and hence we know that (1) and (2) each have precisely two solutions modulo 7 and 11, respectively: $x = \pm 3$ in each case. Again by the Chinese Remainder Theorem, we get four solutions $x_1, \ldots, x_4$ of the original equation, satisfying

$$\begin{array}{ll} x_1 \equiv +3 (\operatorname{mod} 7) & x_1 \equiv +3 (\operatorname{mod} 11) \\ x_2 \equiv +3 (\operatorname{mod} 7) & x_2 \equiv -3 (\operatorname{mod} 11) \\ x_3 \equiv -3 (\operatorname{mod} 7) & x_3 \equiv +3 (\operatorname{mod} 11) \\ x_4 \equiv -3 (\operatorname{mod} 7) & x_4 \equiv -3 (\operatorname{mod} 11) \end{array}$$

Thus, we clearly have $x_1 = 3$ and $x_4 = -3$. To determine x_2, we first use Euclid's algorithm to find $\mathbf{1} = 2 \cdot \mathbf{11} - 3 \cdot \mathbf{7}$; thus,

$22 \equiv 1 (\operatorname{mod} 7)$ and $22 \equiv 0 (\operatorname{mod} 11)$, and $-21 \equiv 0 (\operatorname{mod} 7)$ and $-21 \equiv 1 (\operatorname{mod} 11)$. It follows that $x_2 = 3 \cdot 22 - 3 \cdot (-21) = 129 \equiv 52 \in \mathbb{Z}_{77}$, and $x_3 = -52$. Thus, the four solutions are:

$$\{\pm 3, \pm 52\}.$$

Problem 3. My RSA public key is given by $N = 35$, $e = 5$.

(a) Encrypt the message $[3, 31, 2]$.

Answer: For each $M \in \{3, 18, 2\}$, we have to calculate the element $M^e (\operatorname{mod} N)$. We have $3^5 = 243 \equiv 33 (\operatorname{mod} 35)$, $31^5 \equiv (-4)^5 = -1024 \equiv 26 (\operatorname{mod} 35)$, and $2^5 = 32$. So the encrypted message is $[33, 26, 32]$.

(b) What is my secret decryption key d?

Answer: e and d must satisfy $ed \equiv 1 (\operatorname{mod} \varphi(N))$. In this case, $N = pq$ with $p = 5$ and $q = 7$, thus $\varphi(N) = (p-1)(q-1) = 24$. We use Euclid's algorithm to find the inverse of 5 in $\mathbb{Z}_{24}$, which happens to be $d = 5$.

Problem 4. Consider the following (n, k)-code over the alphabet $A = \mathbb{Z}_2$:

$$C = \{000000, 100011, 010101, 110110, 001110, 101101, 011011, 111000\}.$$

(a) Is this a linear code? If yes, give a generator matrix for it.

Answer: Yes, because C is a subspace of $\mathbb{Z}_2^6$. A possible generator matrix is

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

(b) What are n and k?

Answer: $n = 6$ and $k = 3$.

(c) What is the minimal Hamming distance of this code?

Answer: Since C is a linear code, its minimal Hamming distance is equal to its minimal Hamming weight, which is 3.

(d) How many single-bit errors does this code detect? How many can it correct?

Answer: Since the Hamming distance is 3, this code detects 2 single-bit errors, and it corrects 1

.

(e) Suppose that the following message is received on a noisy channel: 001000, 001100, 110110, 010011. What message was most likely sent?

Answer: We use the nearest neighbor method, looking in each case for a neighbor of Hamming distance 0 or 1. We find 000000, 001110, 110110, 011011.

Problem 5. Find the general solution of the following system of equations in $\mathbb{Z}_2$:

$$\left(\begin{array}{ccccccccccccc} x & & & + & z & + & u & & & & & = & 0 \\ x & + & y & & & + & u & + & v & & & = & 0 \\ x & + & y & + & z & & & & & + & w & = & 0 \end{array}\right)$$

Answer: We use row operations to obtain a row-reduced form.

$$\left[\begin{array}{cccccc|c} 1 & 0 & 1 & 1 & 0 & 0 & 0 \\ 1 & 1 & 0 & 1 & 1 & 0 & 0 \\ 1 & 1 & 1 & 0 & 0 & 1 & 0 \end{array}\right]$$

$$\Longleftrightarrow \left[\begin{array}{cccccc|c} 1 & 0 & 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 1 & 0 & 1 & 0 \end{array}\right] \quad \text{(add r.1 to r.2 and r.3)}$$

$$\Longleftrightarrow \left[\begin{array}{cccccc|c} 1 & 0 & 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 1 & 1 & 0 \end{array}\right] \quad \text{(add r.2 to r.3)}$$

$$\Longleftrightarrow \left[\begin{array}{cccccc|c} 1 & 0 & 0 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 1 & 0 & 1 & 0 \\ 0 & 0 & 1 & 1 & 1 & 1 & 0 \end{array}\right] \quad \text{(add r.3 to r.1 and r.2)}$$

We find that x, y, z are pivot variables and u, v, w are free variables. We let $u = a$, $v = b$, $w = c$, and we find $x = b + c$, $y = a + c$, and $z = a + b + c$. Thus, the most general solution is

$$(x, y, z, u, v, w) = (b + c, a + c, a + b + c, a, b, c),$$

or

$$(x, y, z, u, v, w) = a(0, 1, 1, 1, 0, 0) + b(1, 0, 1, 0, 1, 0) + c(1, 1, 1, 0, 0, 1).$$

Problem 6. In a commutative ring, assume that $a \neq b$, $a^3 = b^3$, and $a^2 b = ab^2$. Prove that $a^2 + b^2$ is not invertible.

Answer: Note that $(a - b)(a^2 + b^2) = a^3 - a^2 b - b^3 + ab^2 = 0$. Thus, if $a^2 + b^2$ were invertible, we would have $a - b = (a - b)(a^2 + b^2)(a^2 + b^2)^{-1} = 0$, contradicting $a \neq b$.

Problem 7. Prove: every finite integral domain is a field.

Answer: Let R be a finite integral domain. This means R is a commutative ring with $|R| > 1$ and with no zero divisors. Let $x \in R$ with $x \neq 0$. We want to show that x is invertible. Consider the function $f : R \to R$ defined by $f(y) = xy$. It is one-to-one by the cancelation property, i.e., if $f(y) = f(y')$, then $xy = xy'$, thus $x(y - y') = 0$, thus $y - y' = 0$ (since x is not a zero divisor). Since f is a function between finite sets of equal cardinality, it follows that f is also onto. Therefore, there exists some y with $f(y) = 1$. But then $xy = 1$, so y is the desired inverse.