MAT 3343, APPLIED ALGEBRA, FALL 2003

Answers to Problem Set 4

Peter Selinger

Problem 1. Let p be prime. We count the number of invertible elements in $\mathbb{Z}_{p^k}$. An element $\bar{x}$ is invertible iff $\gcd(x, p^k) = 1$, iff $p \nmid x$. Thus, the non-invertible elements are precisely the multiples of p, or which there are p^{k-1} in $\mathbb{Z}_{p^k}$. The remaining elements are invertible, and their number is $p^k - p^{k-1} = (p-1)p^{k-1}$.

Problem 2. Find all the divisors of $3+4i$ in $\mathbb{Z}[i]$. Let $z = 3+4i$. If $z = uw$ for some $u, w \in \mathbb{Z}[i]$, then $|u||w| = |z| = 5$, and thus either $|u| \leqslant \sqrt{5}$ or $|w| \leqslant \sqrt{5}$. Thus, for any pair of divisors, one of them has absolute value $\leqslant \sqrt{5}$. Moreover, $u|z$ iff $iu|z$ iff $-u|z$ iff $-iu|z$; thus, we need only check for divisors in the first quadrant. Thus it suffices to check whether the following numbers are divisors:

u	z/u	divisor?	divisors found:
0	undef	no	
1	$3+4i$	yes	$\{1, i, -1, -i, 3+4i, -4+3i, -3-4i, 4-3i\}$
$1+i$	$3.5+0.5i$	no	
$1+2i$	$2.2-0.4i$	no	
2	$1.5+2i$	no	
$2+i$	$2+i$	yes	$\{2+i, -1+2i, -2-i, 1-2i\}$

Problem 3. Suppose R is a ring which satisfies the cancellation property, i.e., whenever $ab = ac$ and $a \neq 0$, then $b = c$. To prove that R is an integral domain, assume that $xy = 0$ and $x \neq 0$. Then $xy = x0$, hence by cancellation, $y = 0$. It follows that R has no zero divisors.

Problem 4. Let $f : \mathbb{C} \to \mathbb{C}$ be the function on complex numbers defined by $f(a+bi) = a - bi$ (complex conjugation). To prove that f is a ring homomorphism, assume that $z = a+bi$ and $w = c+di$ are arbitrary complex numbers. Then:

(a) $f(z+w) = f(a+c+(b+d)i) = a+c-(b+d)i = (a-bi)+(c-di) = f(z)+f(w)$.

(b) $f(0) = f(0+0i) = 0-0i = 0$.

(c) $f(zw) = f((a+bi)(c+di)) = f(ac-bd+(ad+bc)i) = ac-bd-(ad+bc)i = (a-bi)(c-di) = f(z)f(w)$.

(d) $f(1) = f(1+0i) = 1-0i = 1$.

Problem 5. (a) We find the inverse by row operations:

$$\left(\begin{array}{cccc|cccc} 0&1&2&3&1&0&0&0\\ 1&0&4&0&0&1&0&0\\ 0&2&1&3&0&0&1&0\\ 1&4&2&1&0&0&0&1 \end{array}\right)$$

$$\Longleftrightarrow \left(\begin{array}{cccc|cccc} 1&0&4&0&0&1&0&0\\ 0&1&2&3&1&0&0&0\\ 0&2&1&3&0&0&1&0\\ 1&4&2&1&0&0&0&1 \end{array}\right) \quad \text{(exch. rows 1+2)}$$

$$\Longleftrightarrow \left(\begin{array}{cccc|cccc} 1&0&4&0&0&1&0&0\\ 0&1&2&3&1&0&0&0\\ 0&2&1&3&0&0&1&0\\ 0&4&3&1&0&4&0&1 \end{array}\right) \quad \text{(subtract r.1 from r.4)}$$

$$\Longleftrightarrow \left(\begin{array}{cccc|cccc} 1&0&4&0&0&1&0&0\\ 0&1&2&3&1&0&0&0\\ 0&0&2&2&3&0&1&0\\ 0&0&0&4&1&4&0&1 \end{array}\right) \quad \begin{array}{l}\text{(subtract 2$\cdot$ r.2 from r.3),}\\ \text{(add r.2 to r.4)}\end{array}$$

$$\Longleftrightarrow \left(\begin{array}{cccc|cccc} 1&0&0&1&4&1&3&0\\ 0&1&0&1&3&0&4&0\\ 0&0&2&2&3&0&1&0\\ 0&0&0&4&1&4&0&1 \end{array}\right) \quad \begin{array}{l}\text{(subtract r.3 from r.2),}\\ \text{(subtract 2$\cdot$r.3 from r.1)}\end{array}$$

$$\Longleftrightarrow \left(\begin{array}{cccc|cccc} 1&0&0&0&0&0&3&1\\ 0&1&0&0&4&4&4&1\\ 0&0&2&0&0&3&1&2\\ 0&0&0&4&1&4&0&1 \end{array}\right) \quad \begin{array}{l}\text{(add r.4 to r.1 and r.2),}\\ \text{(add 2$\cdot$r.4 to r.3)}\end{array}$$

$$\Longleftrightarrow \left(\begin{array}{cccc|cccc} 1&0&0&0&0&0&3&1\\ 0&1&0&0&4&4&4&1\\ 0&0&1&0&0&4&3&1\\ 0&0&0&1&4&1&0&4 \end{array}\right) \quad \begin{array}{l}\text{(multiply r.3 by 3),}\\ \text{(multiply r.4 by 4)}\end{array}$$

So the inverse matrix is

$$A^{-1} = \begin{pmatrix} 0&0&3&1\\ 4&4&4&1\\ 0&4&3&1\\ 4&1&0&4 \end{pmatrix}.$$

(b) We write the systems as an augmented matrix and solve.

$$\left(\begin{array}{cccc|c} 2 & 1 & 0 & 1 & 2 \\ 1 & 0 & 2 & 0 & 1 \\ 0 & 1 & 2 & 2 & 1 \\ 1 & 2 & 0 & 1 & 0 \end{array}\right)$$

$$\Leftrightarrow \left(\begin{array}{cccc|c} 1 & 2 & 0 & 2 & 1 \\ 1 & 0 & 2 & 0 & 1 \\ 0 & 1 & 2 & 2 & 1 \\ 1 & 2 & 0 & 1 & 0 \end{array}\right) \quad L_1 \leftarrow 2 \cdot L_1$$

$$\Leftrightarrow \left(\begin{array}{cccc|c} 1 & 2 & 0 & 2 & 1 \\ 0 & 1 & 2 & 1 & 0 \\ 0 & 1 & 2 & 2 & 1 \\ 0 & 0 & 0 & 2 & 2 \end{array}\right) \quad L_2 \leftarrow L_2 - L_1, L_3 \leftarrow L_3 - L_1,$$

$$\Leftrightarrow \left(\begin{array}{cccc|c} 1 & 2 & 0 & 2 & 1 \\ 0 & 1 & 2 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 \end{array}\right) \quad L_3 \leftarrow L_3 - L_2, L_4 \leftarrow L_4 + L_3,$$

The answer is more easily written if we continue to row reduced form:

$$\Leftrightarrow \left(\begin{array}{cccc|c} 1 & 0 & 2 & 0 & 1 \\ 0 & 1 & 2 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 \end{array}\right) \quad L_1 \leftarrow L_1 - 2 \cdot L_2$$

$$\Leftrightarrow \left(\begin{array}{cccc|c} 1 & 0 & 2 & 0 & 1 \\ 0 & 1 & 2 & 0 & 2 \\ 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 \end{array}\right) \quad L_2 \leftarrow L_2 - L_3$$

So we have: $w = 1$, $z = a$ is a free variable, $y = 2 - 2a$, $x = 1 - 2a$, thus

$$(x, y, z, w) = (1, 2, 0, 1) + a(-2, -2, 1, 0) = (1, 2, 0, 1) + a(1, 1, 1, 0)$$

Problem 6. (a) 0101010, 1100011, 1001001, 1110000

(b) For each received codeword w, we calculate wH, which is called the *syndrome* of w. w is a valid codeword iff $wH = 0$. Otherwise, the row of H which is equal to wH determines the position of the error.

received word	syndrome	error position	corrected codeword	plaintext
1100110	101	2	1000110	1000
1100011	000	-	1100011	1100
1111000	111	4	1110000	1110
0111110	111	4	0110110	0110
1010101	000	-	1010101	1010

Problem 7. Since $H = \left(\frac{I}{A}\right)$, the generator matrix is $G = (-A|I)$, or

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

(Word processing definitely helps in writing this matrix; it's a lot of work to write it by hand). This is not quite a "systematic" code, because the "parity bits" are attached at the beginning of the codewords, instead of the end.

(a) We encode:

$$\begin{array}{ccc} 01010101010 & \rightarrow & 0101\ 01010101010 \\ 11101110111 & \rightarrow & 0010\ 11101110111 \end{array}$$

(b) There was a typo in the problem: 1000100010001000 has 16 digits, whereas we need 15. So let us decode $v = 100010001000100$. The syndrome is $vH = (0110)$. As this corresponds to the 7th row of H, a single-bit error must have occured in position 7 (assuming that it was indeed a single-bit error, not a multi-bit error, which we cannot correct). So the corrected codeword is 1000 10101000100, corresponding to the plaintext 10101000100.