Solutions to old midterms. Math 228

oldmida.pdf

1. (a) $ax \equiv 1 \pmod{36}$ is solvable iff $(a, 36) = 1$. Since $36 = 2^2 \cdot 3^3$, we need to exclude the numbers that are multiples of 2 and/or 3. We get $a = 1, 5, 7, 11, 13, 17, 19, 23, 25, 29, 31, 35$.

   (b) We need to solve $5x \equiv 1 \pmod{36}$. By simple inspection (or Euclidean algorithm), we get $1 = 35 - 5 \cdot 7$. Then the solution is $x \equiv -7 \pmod{36}$. The corresponding element in S is 29.

2. (a) $115x \equiv 4 \pmod{165}$. We compute $(115, 165) = (5 \cdot 23, 3 \cdot 5 \cdot 11) = 5$. But $5 \not| 4$, therefore the equation does not have solutions.

   (b) $115x \equiv 10 \pmod{165}$. Since $5 | 10$, the equation has 5 solutions. First we do the Euclidean algorithm:

$$165 = 115 + 50$$

$$115 = 50 \cdot 2 + 15$$

$$50 = 15 \cdot 3 + 5$$

$$15 = 5 \cdot 3$$

   We get $5 = 50 - 15 \cdot 3 = 50 - (115 - 50 \cdot 2) \cdot 3 = 50 \cdot 7 - 115 \cdot 3 = (165 - 115) \cdot 7 - 115 \cdot 3 = 165 \cdot 7 - 115 \cdot 10$.

   Thus, $10 = 165 \cdot 14 - 115 \cdot 20$. $x \equiv -20 \pmod{165}$ is a solution. Since $\frac{n}{d} = \frac{165}{5} = 33$. All the solutions are $x \equiv -20, 13, 46, 79, 112 \pmod{165}$.

3. (a) $*$ is an operation since $a * b \in \mathbb{Z}$. (We have not seen this, I won't be asking you a question like this.

   (b) It is associative. $a * (b * c) = a + (b * c) - 7 = a + (b + c - 7) - 7 = (a + b - 7) + c - 7 = (a * b) + c - 7 = (a * b) * c$.

   (c) Take $z = 7$ as identity. Then $a * 7 = a + 7 - 7 = a = 7 * a$.

   (d) Every element has inverse. The inverse for a is $14 - a$. We have $a * (14 - a) = a + 14 - a - 7 = 7$.

4. Let us look at $a^2 + b^2 \equiv c^2 \pmod 3$. We prove the statement by contradiction, so assume that none of a, b, c are divisible by 3. A number a that is not divisible by 3 is either $\equiv 1 \pmod 3$ or $\equiv 2 \pmod 3$. When we square it, we get $a^2 \equiv 1 \pmod 3$ no matter what. Similarly, $b^2, c^2 \equiv 1 \pmod 3$. But then $a^2 + b^2 \equiv c^2 \pmod 3$ becomes $1 + 1 \equiv 1 \pmod 3$ which is a contradiction.

oldmidb.pdf

1. (a) 12 is a unit in $\mathbb{Z}_{19}$ since $(12, 19) = 1$. For its inverse we use the Euclidean algorithm:

$$19 = 12 + 7$$

$$12 = 7 + 5$$

$$7 = 5 + 2$$

$$5 = 2 \cdot 2 + 1$$

$$2 = 1 \cdot 2$$

Therefore, $1 = 5 - 2 \cdot 2 = 5 - (7-5) \cdot 2 = 5 \cdot 3 - 7 \cdot 2 = (12-7) \cdot 3 - 7 \cdot 2 = 12 \cdot 3 - 7 \cdot 5 = 12 \cdot 3 - (19 - 12) \cdot 5 = 12 \cdot 8 - 19 \cdot 5$.

Then 8 is the inverse for 12 in $\mathbb{Z}_{19}$.

(b) Since $12 \cdot 8 = 1$ in $\mathbb{Z}_{19}$, we multiply by 4 to get a solution for $12 \cdot x = 4$ in $\mathbb{Z}_{19}$. Then $x = 32 = 13$ in $\mathbb{Z}_{19}$. (One solution suffices since $(12, 19) = 1$, so there is exactly one solution.

(c) We need a number n that is relatively prime to 2,3,5,7,11,13. We can take, for example, $n = 17$ or 19. Other units would be 4, 6, 9, since they are all relatively primes with n.

2. (a)

$$\begin{pmatrix} a & b \\ 0 & d \end{pmatrix} + \begin{pmatrix} e & f \\ 0 & g \end{pmatrix} = \begin{pmatrix} a+e & b+f \\ 0 & d+g \end{pmatrix} \in S$$

$$\begin{pmatrix} a & b \\ 0 & d \end{pmatrix} \begin{pmatrix} e & f \\ 0 & g \end{pmatrix} = \begin{pmatrix} ae & af+bg \\ 0 & dg \end{pmatrix} \in S$$

Therefore, it is closed under addition and multiplication.

(b) (A regular element is an element that is invertible). Clearly, any multiple of the identity will work. Also any matrix in S with determinant different from zero. For example,

$$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 0 & 2 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 1 & 3 \end{pmatrix}.$$

(c) The zero element is $\begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$, since the sum operation is the one coming from $M_2(\mathbb{R})$. The identity element is $\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ for the same reason.

(d) S is a subring of $M_2(\mathbb{R})$ since the operations are closed, the zero element of $M_2(\mathbb{R})$ belongs to S, and every element of S has its additive inverse in S, since the additive inverse for $\begin{pmatrix} a & b \\ 0 & d \end{pmatrix}$ is $\begin{pmatrix} -a & -b \\ 0 & -d \end{pmatrix}$. Therefore S is a ring.

It is not commutative, since

$$\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 0 & 2 \end{pmatrix} = \begin{pmatrix} 1 & 2 \\ 0 & 2 \end{pmatrix}$$

but

$$\begin{pmatrix} 1 & 0 \\ 0 & 2 \end{pmatrix} \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 0 & 2 \end{pmatrix}$$

Therefore, it is neither an integral domain nor a field.

3. (a) We have not covered this topic yet.

   Notice that a linear combination $45k + 18l$ belongs to I iff k is even, since $18l$ is always even and 45 is odd.

   Since $45k_1 + 18l_1 - (45k_2 + 18l_2) = 45(k_1 - k_2) + 18(l_1 - l_2)$, and k_i even implies that $k_1 - k_2$ is also even, we get that the difference of any two elements in I is an element in I. If $n \in \mathbb{Z}$, then clearly $n(45k + 18l) = 45(kn) + 18(ln) \in I$ since k even implies kn even. Therefore I is an ideal of $\mathbb{Z}$.

   (b) We have not covered this topic yet.

   First notice that the linear combinations of 45 and 18 are generated by $(45, 18) = 9$. We need those numbers that are even. Therefore, we just need the multiples of 18. $I = (18)$. The generators can be written as $18 = 45 \cdot 0 + 18 \cdot 1$.

4. (irreducible here means prime).

   (a) Since $2006p^7|a^2$ and the prime powers dividing a^2 are all even, then p^8 has to divide a^2 and therefore $p^4|a$.

   (b) Take p any prime different from 2, 17, 59. For example, take $p = 3$. Let $a = 2006{\cdot}3$. Then a^2 is divisible by $2006 \cdot 9$ but $9 \not| a$.

5. (a) Since a and b are linear combinations of c and d, we have that $(c, d)|a$ and $(c, d)|b$. Therefore $(c, d)|(a, b)$. Similarly, since c and d are linear combinations of a and b, we have that $(a, b)|c$ and $(a, b)|d$. Therefore $(a, b)|(c, d)$. Then $(a, b) = \pm(c, d)$, and since they are both positive, they must be equal.

   (b) Take $a = 2, b = 3, c = 4, d = 5$. Then $a = 2d - 2c$, $b = 3d - 3c$, $c = 4b - 4a$, and $d = 5b - 5a$.

oldmidc.pdf

1. (a)

$$150 = 71 \cdot 2 + 8$$
$$71 = 8 \cdot 8 + 7$$
$$8 = 7 + 1$$
$$7 = 1 \cdot 7$$

   Then $(150, 71) = 1$. Now $1 = 8-7 = 8-(71-8{\cdot}8) = 8{\cdot}9-71 = (150-71{\cdot}2){\cdot}9-71 = 150 \cdot 9 - 71 \cdot 19$.

   (b) The additive inverse is $-71 = 79$ in $\mathbb{Z}_{150}$. The multiplicative inverse (according to the linear combination we found in (a)) is $-19 = 131$ in $\mathbb{Z}_{150}$.

2. For $n = 1$, we have that $4^1 = 3 \cdot 1 + 1$ in $\mathbb{Z}_9$. Assume the statment is true for $n = k$, i.e., that $4^k = 3k + 1$ in $\mathbb{Z}_9$. Let $n = k + 1$, we have $4^{k+1} = 4 \cdot 4^k = 4 \cdot (3k + 1) = 12k + 4 = 3k + 4 = 3(k + 1) + 1$ in $\mathbb{Z}_9$, which completes the induction.

3. (a) Every integer $n > 1$ can be written in one and only one way in the form $n = p_1 \dots p_r$ where the p_i are positive primes such that $p_1 \leq \dots \leq p_r$.

   (b) Let $(a, b) = 1$. Then there are $u, v \in \mathbb{Z}$ such that $au+bv = 1$. Then $acu+bcv = c$. Since $a|bc$ and $a|acu$, we have that $a|acu + bcv = c$.

4. S is closed for addition and multiplication:

$$(a + b\alpha) + (c + d\alpha) = (a + c) + (b + d)\alpha \in S$$

$$(a+b\alpha)(c+d\alpha) = ac+bd\alpha^2+(bc+ad)\alpha = ac+bd(1+\alpha)+(bc+ad)\alpha = ac+bd+(bd+bc+ad)\alpha \in S$$

Also $0 \in S$. Finally, if $a + b\alpha \in S$, so is $-a - b\alpha \in S$, which is the additive inverse. Therefore S is a subring of R.

5. (a) An integral domain is a commutative ring R with identity $1 \neq 0$ that satisfies the axiom: For every $a, b \in R$, and $ab = 0$, then $a = 0$ or $b = 0$.

   (b) Let e be an idempotent in R, so that $e^2 = e$. Then $e^2 - e = 0$ and $(e - 1)e = 0$. Since R is an integral domain, we must have that either $e - 1 = 0$ (meaning $e = 1$) or $e = 0$.

   (c) Consider $\mathbb{Z}_6$. Then 3 is an idempotent since $3^2 = 9 = 3$ in $\mathbb{Z}_6$.

6. (a) Take $M_2(\mathbb{Z}_2)$, 2×2 matrices with coeffcients in $\mathbb{Z}_2$. This is a ring with the usual matrix operations and it is finite (it has only 16 elements), but is not commutative, since

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

   and

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

   (b) This is not possible that a field is not an integral domain. In a field, every nonzero element has an inverse. If $ab = 0$ and $a \neq 0$, we then multiply by the inverse of a and conclude that $b = 0$. Therefore, it is an integral domain.

   (c) 2, 17, and 34 are three nonzero elements that are not units in $\mathbb{Z}_{68}$, since they have common factors with $68 = 2^2 \cdot 17$.

   (d) Take $a \sim b$ iff $a - b \geq 0$. Then it is reflexive, as $a - a = 0$. It is transitive: if $a \sim b$ and $b \sim c$, then $a - b \geq 0$ and $b - c \geq 0$, so $a - c \geq 0$ and therefore $a \sim c$. However it is not symmetric, for example $2 \sim 1$ but $1 \not\sim 2$.