MAT 3343, APPLIED ALGEBRA, FALL 2003

Answers to Problem Set 2 (due Sept. 30)

Problem 1.2 #17 Proof 1: Suppose $\gcd(m,n)=1$ and $\gcd(k,n)=1$. Let d be a common divisor of mk and n. Suppose that d is divisible by some prime, say $p|d$. Then $p|mk$, hence $p|m$ or $p|k$ by Euclid's Lemma (Thm 6(1), p.41). If $p|m$, then p is a common divisor of m and n, contradicting $\gcd(m,n)=1$. Similarly, if $p|k$, then p is a common divisor of k and n, contradicting $\gcd(k,n)=1$. In either case, we have a contradiction, thus d has no prime factor. It follows that $d=1$ or $d=-1$. In either case, $\gcd(mk,n)=1$.

Proof 2: Suppose $\gcd(m,n)=1$ and $\gcd(k,n)=1$. Let $d=\gcd(mk,n)$, and let $d'=\gcd(d,k)$. Then d' divides k and n, hence $d'=1$ because $\gcd(k,n)=1$. Thus d and k are relatively prime. Since $d|mk$, it follows by Theorem 5(2), p.41, that $d|m$. But also $d|n$, hence $d=1$ since $\gcd(m,n)=1$.

Proof 3: Suppose $\gcd(m,n)=1$ and $\gcd(k,n)=1$. Then, by Euclid's algorithm, there exist x,y,z,w such that $mx+ny=1$ and $kz+nw=1$. Then $\gcd(mk,n)|(mkxz+nkyz+nw)=(mx+ny)kz+nw=kz+nw=1$, hence $\gcd(mk,n)=1$.

Problem 1.2 #18 Suppose $\gcd(m,n)=1$ and $d=\gcd(m+n,m-n)$. Then $d|m+n$ and $d|m-n$, so there exist $a,b\in\mathbb{Z}$ such that $ad=m+n$ and $bd=m-n$. Also, since $\gcd(m,n)=1$, there exist $x,y\in\mathbb{Z}$ such that $xm+yn=1$. We have

$$x(ad+bd)+y(ad-bd)=2xm+2yn=2.$$

But d divides the left-hand-side, thus $d|2$. As 2 is prime, it follows that $d=1$ or $d=2$.

Problem 1.2 #19 Let $d=\gcd(km,kn)$, and let $e=\gcd(m,n)$. We want to show that $d=ke$. First, note that $e|m$ and $e|n$, hence $ke|km$ and $ke|kn$, hence ke is a common divisor of km and kn, hence $ke|d$ (by definition of d. For the converse, use the fact (from Euclid's algorith) that there exist $a,b\in\mathbb{Z}$ such that $e=am+bn$. Then $ke=kam+kbn$. But $d|km$ and $d|kn$, hence $d|kam+kbn$, hence $d|ke$. Because $ke|d$ and $d|ke$, it follows that $ke=\pm d$.

Finally, by definition of gcd, we have assumed that $e,d\geqslant 0$. If we also assume $k\geqslant 0$, then it follows that $ke=d$. Otherwise, if $k<0$, then $ke=-d$, and the statement is false. Thus, problem 1.2 #19 is incorrect; the additional assumption $k\geqslant 0$ should have been made.

Problem 1.2 #24 Let $a=2n+1$ and $b=2n+3$ be two consecutive odd integers. Then $\gcd(a,b)=\gcd(a,b-a)=\gcd(a,2)=\gcd(a-2n,2)=\gcd(1,2)=1$ (by repeated application of Example 3, p.38).

Problem 1.2 #25 Suppose $a=2n+1$, $b=2n+3$, and $c=2n+5$ are three consecutive odd numbers, where $n\geqslant 0$. We claim that if a,b,c are all prime, then $n=1$ and $(a,b,c)=(3,5,7)$. We first prove that one of a,b,c must be divisible by 3. To prove this, consider $\overline{n}\in\mathbb{Z}_3$. There are three cases to consider: Case 1: $\overline{n}=\overline{0}$, in which case $\overline{b}=\overline{2n+3}=\overline{0}$ and $3|2n+3$. Case 2: $\overline{n}=\overline{1}$, in which case $\overline{a}=\overline{2n+1}=\overline{0}$ and $3|2n+1$. Case 3: $\overline{n}=\overline{2}$, in which case $\overline{c}=\overline{2n+5}=\overline{0}$ and $3|2n+5$. In either case, 3 divides one of the numbers a,b,c.

Now if a,b,c are all prime, and one of them is divisible by 3, then this number must actually be *equal* to 3. This leaves two possibilities: $(a,b,c)=(3,5,7)$, $(a,b,c)=(1,3,5)$. The latter triple contains the number 1, which is not prime; therefore $(3,5,7)$ is the only triple of consecutive prime numbers.

Problem 1.3 #19 We want to show that there exists no integer k such that $7|(k^2+1)$. Equivalently, there exists no element $k\in\mathbb{Z}_7$ such that $k^2+\overline{1}=\overline{0}$. Equivalently, there exists no element $k\in\mathbb{Z}_7$ such that $k^2=\overline{-1}=\overline{6}$. There are seven cases to check:

$$\begin{array}{rcl} \overline{-3}^2 &=& \overline{2} \\ \overline{-2}^2 &=& \overline{4} \end{array} \qquad \begin{array}{rcl} \overline{-1}^2 &=& \overline{1} \\ \overline{0}^2 &=& \overline{0} \\ \overline{1}^2 &=& \overline{1} \end{array} \qquad \begin{array}{rcl} \overline{2}^2 &=& \overline{4} \\ \overline{3}^2 &=& \overline{2} \end{array}$$

We see that $\overline{-1}$ is not a square in $\mathbb{Z}_7$.

Problem 1.3 #27 It is helpful to have a table of squares in $\mathbb{Z}_5$, $\mathbb{Z}_7$, and $\mathbb{Z}_9$.

$\mathbb{Z}_5$	$\mathbb{Z}_7$	$\mathbb{Z}_9$
		$\overline{-4}^2 = \overline{7}$
	$\overline{-3}^2 = \overline{2}$	$\overline{-3}^2 = \overline{0}$
$\overline{-2}^2 = \overline{4}$	$\overline{-2}^2 = \overline{4}$	$\overline{-2}^2 = \overline{4}$
$\overline{-1}^2 = \overline{1}$	$\overline{-1}^2 = \overline{1}$	$\overline{-1}^2 = \overline{1}$
$\overline{0}^2 = \overline{0}$	$\overline{0}^2 = \overline{0}$	$\overline{0}^2 = \overline{0}$
$\overline{1}^2 = \overline{1}$	$\overline{1}^2 = \overline{1}$	$\overline{1}^2 = \overline{1}$
$\overline{2}^2 = \overline{4}$	$\overline{2}^2 = \overline{4}$	$\overline{2}^2 = \overline{4}$
	$\overline{3}^2 = \overline{2}$	$\overline{3}^2 = \overline{0}$
		$\overline{4}^2 = \overline{7}$

We solve (a)–(d) by the method of completing the square.

(a) In $\mathbb{Z}_7$:

$$\begin{aligned} x^2+\overline{5}x+\overline{4}=\overline{0} &\iff (x+\overline{6})^2-\overline{6}^2+\overline{4}=\overline{0} \\ &\iff (x+\overline{6})^2=\overline{4} \\ &\iff x+\overline{6}=\overline{2} \text{ or } x+\overline{6}=\overline{-2} \\ &\iff x=\overline{3} \text{ or } x=\overline{6} \end{aligned}$$

(b) In $\mathbb{Z}_5$:

$$\begin{aligned} x^2+\overline{x}+\overline{3}=\overline{0} &\iff (x+\overline{3})^2-\overline{3}^2+\overline{3}=\overline{0} \\ &\iff (x+\overline{3})^2=\overline{1} \\ &\iff x+\overline{3}=\overline{1} \text{ or } x+\overline{3}=\overline{-1} \\ &\iff x=\overline{3} \text{ or } x=\overline{1} \end{aligned}$$

(c) In $\mathbb{Z}_5$:

$$\begin{aligned} x^2+\overline{x}+\overline{2}=\overline{0} &\iff (x+\overline{3})^2-\overline{3}^2+\overline{2}=\overline{0} \\ &\iff (x+\overline{3})^2=\overline{2} \end{aligned}$$

There are no solutions.

(d) In $\mathbb{Z}_9$:

$$\begin{aligned} x^2+\overline{x}+\overline{7}=\overline{0} &\iff (x+\overline{5})^2-\overline{5}^2+\overline{7}=\overline{0} \\ &\iff (x+\overline{5})^2=\overline{0} \\ &\iff x+\overline{5}=\overline{0} \text{ or } x+\overline{5}=\overline{3} \text{ or } x+\overline{5}=\overline{-3} \\ &\iff x=\overline{4} \text{ or } x=\overline{7} \text{ or } x=\overline{1} \end{aligned}$$

(e) Suppose $n\in\mathbb{Z}$ is odd. Then gcd$(n,2)=1$, hence, by Theorem 5, p.54, $\overline{2}$ has an inverse $\overline{r}$ in $\mathbb{Z}_n$. Concretely, we can let $r=(n+1)/2$, which is an integer, and we find that $\overline{2}\cdot\overline{r}=\overline{n+1}=\overline{1}$. For the next claim, we use completion of the square: for all $x\in\mathbb{Z}_n$, we have

$$\begin{aligned} x^2+\overline{a}x+\overline{b}=\overline{0} &\iff x^2+\overline{2}\overline{r}\,\overline{a}x+\overline{b}=\overline{0} \\ &\iff (x+\overline{r}\,\overline{a})^2-\overline{r}^2\overline{a}^2+\overline{b}=\overline{0} \\ &\iff (x+\overline{r}\,\overline{a})^2=\overline{r}^2\overline{a}^2-\overline{b}. \end{aligned}$$

This has a solution iff the right-hand-side $\overline{r}^2\overline{a}^2-\overline{b}$ is a square in $\mathbb{Z}_n$.

Problem 3.1 #4 We use the subring test (Thm 5, p.194). Suppose that S,T are subrings of R. To show that $S\cap T$ is a subring, we check conditions (1) and (2).

But $0\in S$ and $0\in T$, hence $0\in S\cap T$; similarly $1\in S$ and $1\in T$, hence $1\in S\cap T$. Thus, $S\cap T$ satisfies (1). For (2), suppose $s,t\in S\cap T$. Then $s,t\in S$, hence $s+t,st,-s\in S$ because S is a subring. Also, $s,t\in T$, hence $s+t,st,-s\in T$ because T is a subring. It follows that $s+t,st,-s\in S\cap T$. Hence $S\cap T$ is a subring.

In general, $S+T$ is not a subring of R, even if S and T are subrings. Consider, for example, $R=\mathbb{Z}[x,y]$, the ring of polynomials in two variables, and let $S=\mathbb{Z}[x]$ and $T=\mathbb{Z}[y]$ be the subrings of polynomials which only use the variable x and y, respectively. Then $S+T$ is the set of polynomials of the form

$$a_0+b_1x+b_2x^2+b_3x^3+\ldots+c_1y+c_2y^2+c_3y^3+\ldots,$$

i.e., polynomials which only contain powers of x and powers of y (but no mixed powers). Then $x\in S+T$ and $y\in S+T$, but $xy\notin S+T$. Therefore, $S+T$ is not a subring.

Problem 3.1 #10 Suppose R is a ring, $a,b\in R$, and $ab+ba=1$ and $a^3=a$. Multiplying the equation $ab+ba=1$ by a from the left and right, we get $a(ab+ba)a=a1a$, hence, by using the ring axioms, $a^2ba+aba^2=a^2$. Also, plugging $a^3=a$ into $ab+ba=1$, we get $a^3b+ba^3=1$. Then:

$$\begin{aligned} 1+a^2 &= (a^3b+ba^3)+(a^2ba+aba^2) \\ &= a^3b+a^2ba+ba^3+aba^2 \\ &= a^2(ab+ba)+(ba+ab)a^2 \quad = \quad a^2+a^2. \end{aligned}$$

Subtracting a^2 from both sides of the equation, we obtain $1=a^2$. NOTE: we have not used commutativity of multiplication anywhere; thus, this result is true in any ring, not just in a commutative ring.

Problem 3.1 #18 (a) The characteristic of $\mathbb{Z}_n\times\mathbb{Z}_m$ is the smallest positive integer k such that $k(\mathbb{Z}_n\times\mathbb{Z}_m)=0$ (or 0 if no such positive integer exists). But $k(\mathbb{Z}_n\times\mathbb{Z}_m)=k\mathbb{Z}_n\times k\mathbb{Z}_m=0$ iff $k\mathbb{Z}_n=0$ and $k\mathbb{Z}_m=0$, iff $n|k$ and $m|k$, iff $\mathrm{lcm}(n,m)|k$. Thus, char$(\mathbb{Z}_n\times\mathbb{Z}_m)=\mathrm{lcm}(n,m)$.

More generally, we have char$(R\times S)=\mathrm{lcm}(\mathrm{char}\,R,\mathrm{char}\,S)$.

(b) Note that, as an additive group, $M_2(R)$ is isomorphic to $R\times R\times R\times R$, via the isomorphism $\varphi\begin{pmatrix} a & b \\ c & d\end{pmatrix}=(a,b,c,d)$. The characteristic of a ring only depends on the underlying additive group, thus char$(M_2(R))=$ char$(R^4)=$ char(R). In particular, char$(M_2(\mathbb{Z}_n))=n$.

(c) char$(\mathbb{Z}\times\mathbb{Z}_n)=\mathrm{lcm}(\mathrm{char}\,\mathbb{Z},\mathrm{char}\,\mathbb{Z}_n)=\mathrm{lcm}(0,n)=0$.