MAT 312/AMS 351: Applied Algebra
Solutions to Midterm I (70pts)

Problem 1 (5pts)

Suppose $a, b \in \mathbb{Z}^+$ *are two positive integers such that*

$$2a - 3b = 5.$$

(a) *There are two possibilities for* $\gcd(a, b)$. *What are they?* **Answer Only.**

$$\boxed{\gcd(a, b) = \quad 1 \quad \text{or} \quad 5}$$

(b) *Explain* why there are no other possibilities.

$\gcd(a, b)$ must divide $2a - 3b = 5$.

(c) *Give an example of a pair* (a, b) *for each of the two possibilities in (a).* **Answer Only.**

$$\boxed{\text{Possibility 1 in (a): } (a, b) = (\ 4\ ,\ 1\ )}$$

$$\boxed{\text{Possibility 2 in (a): } (a, b) = (\ 10\ ,\ 5\ )}$$

Grading: ✓ if completely correct; X otherwise on each part; 1 point for each of 4 correct answers in (a) and (c); other answers are possible in (c); 1 point for (b); -1 for each answer containing a non-integer number; total score = number of ✓ *minus* number of -1

Problem 2 (3+7pts)

Define a sequence $a_1, a_2, a_3, \ldots$ *by*

$$a_1 = 1, \qquad a_2 = 2, \qquad \text{and} \qquad a_{n+2} = a_n^2 + a_{n+1} \quad \forall\, n \geq 1.$$

(a) *Determine the first 5 numbers,* a_n *with* $n = 1, \ldots, 5$*, in this sequence. The answer must appear in the box below; no explanation is required for this part.*

1, 2, 3, 7, 16

Grading: a_1, a_2, a_3 correct 1pt; a_4 based on a_2, a_3 1pt; a_5 based on a_3, a_4 1pt

(b) *Prove that every two successive terms in this sequence,* a_n *and* a_{n+1}*, are relatively prime.*

We use induction. Since

$$\gcd\left(a_1, a_{1+1}\right) = \gcd(1, 2) = 1,$$

the claim holds in the base $n = 1$ case. If the claim holds for some $n \geq 1$, then $\gcd(a_{n+1}, a_n^2) = 1$ and

$$\gcd\left(a_{n+1}, a_{(n+1)+1}\right) = \gcd\left(a_{n+1}, a_n^2 + a_{n+1}\right) = \gcd\left(a_{n+1}, a_n^2\right) = 1;$$

the second equality above holds because adding a multiple of the first input to the second does not change the gcd of the two inputs. Thus, the claim holds for $n+1$. This completes the proof.

Note: it is not the case in general that $\gcd(a, b^2) = \gcd(a, b)$, e.g. this is not true for $a = 4$ and $b = 2$. This identity is true if $\gcd(a, b) = 1$ because in this case a and b have no prime factors in common.

Grading: proper inductive setup 1pt; base case 1pt; reason for $\gcd(a_{n+1}, a_n^2) = 1$ 3pts (no credit for just stating that it equals $\gcd(a_{n+1}, a_n)$); rest of inductive step 2pts

Problem 3 (8+4pts)

Show and explain your work clearly below.

(a) *Find* $\gcd(11,64)$ *and express it in the form* $11s+64t$ *for some* $s,t\in\mathbb{Z}$.

We use Euclid's algorithm, first with non-matrix version:

$$\begin{aligned}
&(1):\ \mathbf{64}=5\cdot\mathbf{11}+\mathbf{9} && \gcd(11,64)=\mathbf{1}\overset{(3)}{=}\mathbf{9}-4\cdot\mathbf{2}\\
&(2):\ \mathbf{11}=1\cdot\mathbf{9}+\mathbf{2} && \overset{(2)}{=}\mathbf{9}-4\cdot(\mathbf{11}-1\cdot\mathbf{9})=5\cdot\mathbf{9}-4\cdot\mathbf{11}\\
&(3):\ \ \mathbf{9}=4\cdot\mathbf{2}+\mathbf{1} && \overset{(1)}{=}5\cdot(\mathbf{64}-5\cdot\mathbf{11})-4\cdot\mathbf{11}=5\cdot\mathbf{64}-29\cdot\mathbf{11}
\end{aligned}$$

Thus, $\gcd(11,64)=\boxed{1=5\cdot\mathbf{64}+(-29)\cdot\mathbf{11}}$

Now the matrix version.

$$\left(\begin{array}{cc|c}1&0&11\\0&1&64\end{array}\right)\longrightarrow\left(\begin{array}{cc|c}1&0&11\\-5&1&9\end{array}\right)\longrightarrow\left(\begin{array}{cc|c}6&-1&2\\-5&1&9\end{array}\right)\longrightarrow\left(\begin{array}{cc|c}6&-1&2\\-29&5&1\end{array}\right).$$

The second matrix is obtained from the first by subtracting the first row (which has the smaller last entry 11) times 5 from the second row (largest multiple of 11 dividing the last entry in the second row 64). The third matrix is obtained from the second by subtracting the second row from the first row. The fourth matrix is obtained from the third by subtracting the first row times 4 from the second row. Since the last entry in the second row of the fourth matrix divides all other entries, this entry is $\gcd(11,64)$ and this row gives $\gcd(11,64)=\boxed{1=-29\cdot11+5\cdot64}$

The computation above is a shorthand for

$$\begin{aligned}
\begin{pmatrix}1&0\\0&1\end{pmatrix}\begin{pmatrix}11\\64\end{pmatrix}=\begin{pmatrix}11\\64\end{pmatrix}&\longrightarrow\begin{pmatrix}1&0\\-5&1\end{pmatrix}\begin{pmatrix}11\\64\end{pmatrix}=\begin{pmatrix}11\\9\end{pmatrix}\\
&\longrightarrow\begin{pmatrix}6&-1\\-5&1\end{pmatrix}\begin{pmatrix}11\\64\end{pmatrix}=\begin{pmatrix}2\\9\end{pmatrix}\\
&\longrightarrow\begin{pmatrix}6&-1\\-29&5\end{pmatrix}\begin{pmatrix}11\\64\end{pmatrix}=\begin{pmatrix}2\\1\end{pmatrix}.
\end{aligned}$$

Grading: $\gcd(11,64)$ 1pt; as integer linear combination 2pt; explanation 5pts; −8pts for the question if any non-integer numbers appear, regardless of anything else

(b) *Find the inverse of 11 mod 64 (the answer should be an integer between 0 and 63).*

By (a), $(-29)\cdot11\equiv1 \bmod 64$. Thus, the inverse 11 mod 64 is -29, which is the same as

$$-29+64=\boxed{35}\mod 64.$$

Grading: −29 2pts; 35 1pt; nominal explanation 1pt; −4pts for the question if any non-integer numbers appear, regardless of anything else; no penalty for carryover errors from (a)

Problem 4 (12pts)

A public key code has base 85 and exponent 11, i.e. $m \equiv \beta^{11}$ mod 85 is the message determined by a block β being encoded. The encoded message received is 81. Decode this message. Show and explain your work clearly.

Since $85 = 5 \cdot 17$ and $5, 17$ are distinct primes,

$$\big|G_{85}\big| = \big|G_{5\cdot 17}\big| = \big|G_5\big| \cdot \big|G_{17}\big| = \big(5^1 - 5^0\big)\big(17^1 - 17^0\big) = 64.$$

We need to find x such that $\beta^{11x} \equiv \beta^1$ mod 85 whenever $\gcd(\beta, 1) = 85$. By Euler's Theorem and the above equation, this is the case if $11x + 64k = 1$ for some $k \in \mathbb{Z}$. By Problem 3a, $(x, k) = (-29, 5)$ satisfies this condition and thus so does

$$(x, k) = \big(-29 + 64, 5 - 11\big) = (35, -6).$$

From this, we conclude that the decoding power $x = 35$. Alternatively, x should be the inverse of 11 mod 64, which is provided by Problem 3b. The decoding of the message is then

$$\beta \equiv m^x \equiv 81^{35} \equiv (-4)^{35} \equiv -(2^2)^{35} \equiv -2^{70} \equiv -2^{64} \cdot 2^6 \equiv -1 \cdot 64 \equiv \boxed{21} \mod 85;$$

the penultimate identity follows from Euler's theorem.

Grading: $|G_{85}|$ 3pts; correct x 3pts; 81^{35} 1pt; nominal explanation 1pt; up to 4pts for simplifying 81^{35}; direct use of the answers in Problem 3 is fine; no penalty for carryover errors from Problem 3; -6pts for the question if any non-integer numbers appear, regardless of anything else

Problem 5 (5+5+5pts)

Show and explain your work clearly below.

(a) *Let p be an odd prime. How many distinct solutions $x \in \mathbb{Z}_p$ does the equation*

$$x^2 = [1]_p$$

have?

If $x = [a]_p$, the above equation is equivalent to

$$\big(x-[1]_p\big)\big(x+[1]_p\big) = 0 \in \mathbb{Z}_p \qquad \Longleftrightarrow \qquad p\,\big|\,\big(a-1\big)\big(a+1\big) = 0.$$

Since p is prime, it follows that either $p|(a-1)$ (and so $x=[1]_p$) or $p|(a+1)$ (and so $x=-[1]_p$). Since $p>2$, $[1]_p \neq -[1]_p$ and so the equation has $\boxed{2}$ distinct roots.

Grading: correct answer 1pt; explanation 4pts; negative points for non-integer expressions

(b) *Let p be an odd prime. How many elements does the subset*

$$\big\{x^2 : x \in \mathbb{Z}_p\big\} \subset \mathbb{Z}_p$$

contain?

The idenity $[a]_p^2 = [b]_p^2$ is equivalent

$$\big([a]_p-[b]_p\big)\big([a]_p+[b]_p\big) = 0 \in \mathbb{Z}_p \qquad \Longleftrightarrow \qquad p\,\big|\,\big(a-b\big)\big(a+b\big) = 0.$$

Since p is prime, it follows that either $p|(a–b)$ (and so $[a]_p = [b]_p$) or $p|(a+b)$ (and so $[a]_p = -[b]_p$). If $[a]_p = -[a]_p$, then $p|(2a)$ and thus $p|a$ (and so $[a]_p = [0]_p$). Thus, the set of squares above contains $[0]_p = [0]_p^2$. All other elements of this set come from a pair of distinct elements of $\mathbb{Z}_p - \{[0]_p\}$. Thus, the total number of squares is

$$1 + \frac{p-1}{2} = \boxed{\frac{p+1}{2}}$$

Grading: correct answer 1pt; explanation 4pts; negative points for non-integer expressions

(c) *Let p and q be distinct odd primes. How many distinct solutions $x \in \mathbb{Z}_{pq}$ does the equation*

$$x^2 = [1]_{pq}$$

have?

Let $x = [a]_{pq}$. Since p and q are relatively prime, by the Chinese Remainder Theorem the above equation is equivalent to

$$\begin{cases} a^2 \equiv 1 \mod p \\ a^2 \equiv 1 \mod q \end{cases} \qquad \Longleftrightarrow \qquad \begin{cases} a \equiv \pm 1 \mod p \\ a \equiv \pm 1 \mod q \end{cases}$$

the last equivalence is established in (a). By the Chinese Remainder Theorem again, each of the four pairs $(a,a) \equiv (\pm 1, \pm 1) \mod (p,q)$ corresponds to an element $x \in \mathbb{Z}_{pq}$ solving the original equation.

Grading: correct answer 1pt; explanation 4pts; negative points for non-integer expressions

Problem 6 (4+8+4pts)

Solve the linear congruences and systems of congruences below. Show and explain your work clearly.

(a) $3x+5 \equiv x-3 \bmod 7$

This is the same as $2x \equiv -1 \bmod 7$. Multiplying both sides by 4, we obtain $8x \equiv -4 \bmod 7$. This is the same as $\boxed{x \equiv 3 \bmod 7}$

Grading: correct answer 3pts (as a congruence class is fine); nominal explanation 1pt; wrong answer 0pts for the question if no non-integer number appears; −4pts for the question if any non-integer numbers appear, regardless of anything else.

(b) $\begin{cases} 3x+5 \equiv x-3 & \bmod 7 \\ 2x \equiv 4 & \bmod 8 \end{cases}$

By part (a), this is the same as $\begin{cases} x \equiv 3 & \bmod 7 \\ 2x \equiv 4 & \bmod 8 \end{cases}$

The second equation implies that $x \equiv 2 \bmod 4$ and has two solutions mod 8, 2 and 2+4. The first equation means that $x = 3+7k$ for some $k \in \mathbb{Z}$. So, we need to find k such that

$$3+7k \equiv 2, 6 \bmod 8, \qquad -k \equiv -1, 3 \bmod 8, \qquad k \equiv 1, -3 \bmod 8.$$

Thus, $\boxed{x \equiv 10, -18 \equiv 10, 38 \bmod 56}$

Alternatively, $(-1)\cdot 7+1\cdot 8=1$. As stated in the book, this implies that

$$(-1)\cdot 7\cdot 2+1\cdot 8\cdot 3 = 10 \quad \text{and} \quad (-1)\cdot 7\cdot 6+1\cdot 8\cdot 3 = -18 \equiv 38$$

are the mod 56 solutions of this system.

Grading: $x \equiv 10$ as the only mod 28 solution of this system also acceptable; correct number of solutions 2pts; correct solutions 2pts; explanation up to 4pts, even if the answer is wrong; −8pts for the question if any non-integer numbers appear, regardless of anything else.

(c) $\begin{cases} 3x+5 \equiv x-3 & \bmod 7 \\ 2x \equiv 4 & \bmod 8 \\ 3x \equiv 5 & \bmod 9 \end{cases}$

Since $\gcd(3, 9) = 3$ does not divide 5, the last equation has no solutions. Thus, the system has $\boxed{\text{no solutions}}$

Grading: correct answer 2pts; explanation 2pts; wrong answer 0pts for the question if no non-integer number appears; −4pts for the question if any non-integer numbers appear, regardless of anything else.