MATH 135 Algebra, Solutions to the Final Exam, Fall 2009

[6] **1:** (a) Let $a_0 = 1$ and $a_1 = 3$, and for $n \geq 2$ let $a_n = 3a_{n-1} - 2a_{n-2} - 1$. Show that $a_n = 2^n + n$ for all $n \geq 0$.

Solution: We claim that $a_n = 2^n + n$ for all $n \geq 0$. When $n = 0$ we have $a_n = a_0 = 1$ and $2^n + n = 2^0 + 0 = 1$, and when $n = 1$ we have $a_n = a_1 = 3$ and $2^n + n = 2^1 + 1 = 3$, so the claim is true when $n = 0$ and when $n = 1$. Let $k \geq 3$ and suppose the claim is true when $n = k-1$ and when $n = k-2$, that is suppose $a_{k-1} = 2^{k-1} + k - 1$ and $a_{k-2} = 2^{k-2} + k - 2$. Then when $n = k$ we have

$$\begin{aligned} a_n = a_k &= 3a_{k-1} - 2a_{k-2} - 1 = 3\left(2^{k-1} + k - 1\right) - 2\left(2^{k-2} + k - 2\right) - 1 \\ &= 3 \cdot 2^{k-1} + 3k - 3 - 2^{k-1} - 2k + 4 - 1 = 2 \cdot 2^{k-1} + k = 2^k + k = 2^n + n \,. \end{aligned}$$

Thus the claim is true when $n = k$, and so by Mathematical Induction, the claim is true for all $n \geq 0$.

[4] (b) Find the term containing x^8 in the binomial expansion of $\left(\frac{18}{x} - \frac{x^2}{3}\right)^7$.

Solution: The i^{th} term in the expansion is

$$\binom{7}{i}\left(\frac{18}{x}\right)^{7-i}\left(-\frac{x^2}{3}\right)^i = (-1)^i\binom{7}{i}\left(\frac{18^{7-i}}{3^i}\right)x^{3i-7} \,.$$

To get $3i - 7 = 8$ we need $3i = 15$, that is $i = 5$. The 5^{th} term in the expansion is

$$(-1)^5\binom{7}{5}\left(\frac{18^2}{3^5}\right)x^8 = -\frac{7 \cdot 6}{2} \cdot \frac{2^2 \cdot 3^4}{3^5}\,x^8 = -28\,x^8 \,.$$

[3] **2:** (a) Let $a = -215$ and $b = 17$. Find the integers q and r wth $0 \leq r < b$ such that $a = qb + r$.

Solution: Using long division, we have $215 = 12 \cdot 17 + 11$, so $-215 = -12 \cdot 17 - 11 = -13 \cdot 17 + 6$, so we take $q = -13$ and $r = 6$.

[7] (b) List all pairs of integers (x, y) with $|x| \leq 50$ such that $245x + 189y = 84$.

Solution: The Euclidean Algorithm gives

$$245 = 1 \cdot 189 + 56 \ , \quad 189 = 3 \cdot 56 + 21 \ , \quad 56 = 2 \cdot 21 + 14 \ , \quad 21 = 1 \cdot 14 + 7 \ , \quad 14 = 2 \cdot 7 + 0$$

so we have $\gcd(245, 189) = 7$. Then Back-Substitution gives the sequence

$$1 \ , \ 1 \ , \ 3 \ , \ -10 \ , \ 13$$

so we have $(245)(-10) + (189)(13) = 7$. Multiplying by $\frac{84}{7} = 12$ gives $(245)(-120) + (189)(156) = 84$, so one solution is $(x, y) = (-120, 156)$. Note that $\frac{245}{7} = 35$ and $\frac{189}{7} = 27$, so by the Linear Diophantine Equation Theorem, the general solution is

$$(x, y) = (-120, 156) + k(27, -35) \ , \quad k \in \mathbf{Z} \,.$$

We have

$$\begin{aligned} |x| \leq 50 &\iff -50 \leq x \leq 50 \iff -50 \leq -120 + 27k \leq 50 \iff 70 \leq 27k \leq 170 \\ &\iff \left\lceil \tfrac{70}{27} \right\rceil \leq k \leq \left\lfloor \tfrac{170}{27} \right\rfloor \iff 3 \leq k \leq 6 \,, \end{aligned}$$

Thus the solutions with $|x| \leq 50$ are $(x, y) = (-120, 156) + k(27, -35)$ with $k \in \{3, 4, 5, 6\}$, that is

$$(x, y) = (-39, 51), (-12, 16), (15, -19), (42, -54) \,.$$

[4] **3:** (a) List all elements $[x] \in \mathbf{Z}_{13}$ such that $[5][x]^2 = [6]$.

Solution: We make a table of values modulo 13.

x	0	1	2	3	4	5	6	7	8	9	10	11	12
x^2	0	1	4	9	3	12	10	10	12	3	9	4	1
$5x^2$	0	5	7	6	2	8	11	11	8	2	6	7	5

From the table we see that $5x^2 \equiv 6 \pmod{13}$ if and only if $x \equiv 3$ or $10 \pmod{13}$, and so in $\mathbf{Z}_{13}$ we have $[5][x]^2 = [6] \iff [x] = [3]$ or $[10]$.

[6] (b) Solve the pair of congruences $x \equiv 5 \pmod 9$ and $10x \equiv 6 \pmod{28}$.

Solution: By dividing all terms by 2 then multiplying both sides by 3, we see that

$$10x \equiv 6 \pmod{28} \iff 5x \equiv 3 \pmod{14} \iff x \equiv 9 \pmod{14}.$$

To get $x \equiv 5 \pmod 9$ and $x \equiv 9 \pmod{14}$ we must have $x = 5 + 9r$ and $x = 9 + 14s$ for some integers r and s, so we need $5 + 9r = 9 + 14s$, that is $9r - 14s = 4$. By inspection, one solution to this equation is $(r, s) = (2, 1)$, and so one solution for the pair of congruences is $x = 5 + 9r = 5 + 9 \cdot 2 = 23$. Note that $9 \cdot 14 = 126$, so by the Chinese Remainder Theorem, the general solution is

$$x \equiv 23 \pmod{126}.$$

[5] **4:** (a) Use the Square and Multiply Algorithm to encrypt the message $m = 4$ using the RSA public key $(n, e) = (253, 29)$.

Solution: We make a list of powers of $m = 4$ modulo $n = 253$.

k	4^k
1	4
2	16
4	3
8	9
16	81

Note that $29 = 16 + 8 + 4 + 1$ so we have

$$c \equiv m^e \equiv 4^{29} \equiv 4^{16} \cdot 4^8 \cdot 4^4 \cdot 4^1 \equiv 81 \cdot 9 \cdot 3 \cdot 4 \equiv 146 \pmod{253}$$

so the cyphertext is $c = 146$.

[5] (b) Determine the private key (n, d) which corresponds to the public key $(n, e) = (253, 29)$.

Solution: Note that $n = 253 = 11 \cdot 23$ so that $\phi(n) = \phi(11)\phi(23) = 10 \cdot 22 = 220$. The value of d in the public key is given by $d = e^{-1} \big(\bmod\ \phi(n)\big)$, that is $d = 29^{-1} \pmod{220}$. We consider the equation $29x + 220y = 1$. The Euclidean Algorithm gives

$$220 = 7 \cdot 29 + 17\ , \quad 29 = 1 \cdot 17 + 12\ , \quad 17 = 1 \cdot 12 + 5\ , \quad 12 = 2 \cdot 5 + 2\ , \quad 5 = 2 \cdot 2 + 1$$

so we have $\gcd(29, 220) = 1$, and then Back-Substitution gives

$$1\ , \quad -2\ , \quad 5\ , \quad -7\ , \quad 12\ , \quad -91$$

so we have $(29)(-91) + (220)(12) = 1$. Thus $29^{-1} \equiv -91 \equiv 129 \pmod{220}$, so we can take $d = 129$. (Alternatively, we can use $d = e^{-1} \big(\bmod\ \psi(n)\big)$, where $\psi(n) = \operatorname{lcm}\big(\phi(11), \phi(23)\big) = \operatorname{lcm}(10, 22) = 110$). By a calculation similar to the one above, we obtain $d = 19$).

[2] **5:** (a) Define $\phi(n)$, where n is a positive integer and ϕ is the Euler phi function.

Solution: For a positive integer n, $\phi(n)$ is the number of integers a with $1 \leq a \leq n$ such that $\gcd(a,n)=1$. Equivalently, $\phi(n)$ is the number of invertible elements in $\mathbf{Z}_n$.

[3] (b) State the Chinese Remainder Theorem.

Solution: The Chinese Remainder Theorem states that for all $a,b,n,m \in \mathbf{Z}$, if $\gcd(n,m)=1$ then the pair of congruences $x \equiv a \pmod{n}$ and $x \equiv b \pmod{m}$ has a solution, and that if $x=u$ is one solution then the general solution is $x \equiv u \pmod{nm}$.

[5] (c) Let $n=pq$ where p and q are distinct primes, and let $\phi=\phi(n)=(p-1)(q-1)$. Prove that for all integers a we have $a^{\phi+1} \equiv a \pmod{n}$. (This is part of Proposition 7.41).

Solution: Let $a \in \mathbf{Z}$. If $p \big| a$ then we have $a \equiv 0 \equiv a^{\phi+1} \pmod{p}$. If $p \not\big| a$ then by Fermat's Little Theorem we have $a^{p-1} \equiv 1 \pmod{p}$ so $a^{\phi} \equiv a^{(p-1)(q-1)} \equiv \left(a^{p-1}\right)^{q-1} \equiv 1^{q-1} \equiv 1 \pmod{p}$ and hence $a^{\phi+1} \equiv a \pmod{p}$. In both cases we have $a^{\phi+1} \equiv a \pmod{p}$. Similarly, we have $a^{\phi+1} \equiv a \pmod{q}$ and so by the Chinese Remainder Theorem, $a^{\phi+1} \equiv a \pmod{n}$.

[5] **6:** (a) Determine the number of positive integers a such that $a \big| 9!$ and $\gcd(a,3600)=180$.

Solution: Note that $9! = 9\cdot 8\cdot 7\cdot 6\cdot 5\cdot 4\cdot 3\cdot 2 = 3^2\cdot 2^3\cdot 7\cdot 2\cdot 3\cdot 5\cdot 2^2\cdot 3\cdot 2 = 2^7\cdot 3^4\cdot 5^1\cdot 7^1$, so to get $a \big| 9!$, we must have $a = 2^i\cdot 3^j\cdot 5^k\cdot 7^l$ for some integers i,j,k,l with $0 \leq i \leq 7$, $0 \leq j \leq 4$, $0 \leq k \leq 1$ and $0 \leq l \leq 1$. Then we have

$$\gcd(a,3600) = \gcd(2^i\,3^j\,5^k\,7^l, 2^4\,3^2\,5^2) = 2^{\min(i,4)}\cdot 3^{\min(j,2)}\cdot 5^{\min(k,2)}$$

so to get $\gcd(a,3600)=180=2^2\,3^2\,5^1$ we need $\min(i,4)=2$ so $i=2$, and $\min(j,2)=2$ so $j\in\{2,3,4\}$, and $\min(k,2)=1$ so $k=1$. Since there is 1 choice for i, 3 choices for j, 1 choice for k and 2 choices for l, there are $1\cdot 3\cdot 1\cdot 2=6$ such integers a.

[5] (b) Prove that $\gcd\left(5^{98}+3, 5^{99}+1\right)=14$.

Solution: Recall that if $a=qb+r$ then $\gcd(b,a)=\gcd(b,r)$. Since $(2^{99}+1)=(5)(2^{98}+3)-14$, we have

$$\gcd\left(5^{98}+3, 5^{99}+1\right) = \gcd\left(5^{98}+3, -14\right) = \gcd\left(5^{98}+3, 14\right).$$

Note that $2\big|(5^{98}+3)$ since 5^{98} is odd and 3 is odd. Also, by Fermat's Little Theorem the list of powers of 5 repeats every 6 terms modulo 7, and we have $98 \equiv 2 \pmod{6}$, so $5^{98}+3 \equiv 5^2+3 \equiv 28 \equiv 0 \pmod{7}$, that is $7\big|(5^{98}+3)$. Since $2\big|(5^{98}+3)$ and $7\big|(5^{98}+3)$, we have $14\big|(5^{98}+3)$, and hence $\gcd\left(5^{98}+3, 14\right)=14$.

[3] **7:** (a) Simplify $z = \dfrac{(1+3i)^2 + (5-i)}{(1+i)}$.

Solution: We have $z = \dfrac{(1+3i)^2 + (5-i)}{(1+i)} = \dfrac{(-8+6i)+(5-i)}{1+i} = \dfrac{-3+5i}{1+i} \cdot \dfrac{1-i}{1-i} = \dfrac{2+8i}{2} = 1 + 4i\,.$

[3] (b) Solve $z = \dfrac{1+8i}{2-z}$ for $z \in \mathbf{C}$.

Solution: Note that $w^2 = -8i = 8e^{-i\,\pi/2} \iff w = \pm 2\sqrt{2}\,e^{-i\,\pi/4} = \pm 2\sqrt{2}\left(\frac{1}{\sqrt{2}} - \frac{1}{\sqrt{2}}i\right) = \pm(2-2i)$. Using the Quadratic Formula, we have

$$\begin{aligned}
z = \frac{1+8i}{2-z} &\iff z(2-z) = 1+8i \iff 2z - z^2 = 1+8i \iff z^2 - 2z + (1+8i) = 0 \\
&\iff z = \frac{2 \pm \sqrt{4 - 4(1+8i)}}{2} = 1 \pm \sqrt{1-(1+8i)} = 1 \pm \sqrt{-8i} = 1 \pm (2-2i) \\
&\iff z = 3 - 2i \text{ or } -1 + 2i\,.
\end{aligned}$$

[4] (c) Solve $z^5 + 16\,\overline{z} = 0$ for $z \in \mathbf{C}$. Draw a picture showing all of the solutions.

Solution: Let $z = re^{i\,\theta}$. Then we have

$$\begin{aligned}
z^5 + 16\overline{z} = 0 &\iff \left(re^{i\,\theta}\right)^5 + 16\,\overline{re^{i\,\theta}} \iff r^5 e^{i\,5\theta} + 16re^{-i\,\theta} = 0 \\
&\iff \left(r = 0 \text{ or } r^4 e^{i\,6\theta} = -16 = 16e^{i\,\pi}\right) \\
&\iff \left(r = 0 \text{ or } \left(r = 2 \text{ and } 6\theta = \pi + 2\pi k\ , \text{ for some } k \in \mathbf{Z}\right)\right) \\
&\iff \left(r = 0 \text{ or } \left(r = 2 \text{ and } \theta = \tfrac{\pi}{6} + \tfrac{\pi}{3}k \text{ for some } k \in \{0,1,2,3,4,5\}\right)\right) \\
&\iff z \in \left\{0, 2e^{i\,\pi/6}, 2e^{i\,\pi/2}, 2e^{i\,5\pi/6}, 2e^{i\,7\pi/6}, 2e^{i\,3\pi/2}, e^{i\,11\pi/6}\right\}
\end{aligned}$$

In cartesian coordinates, the solutions are $z = 0, \pm 2i, \pm\sqrt{3} \pm i$. We omit the picture.