18.781 Exam 2 Solutions - Fall 2008

Problem 1. (*Short answer; 5 pts each*) Unless asked otherwise, you are not required to show detailed work for these questions, and need only give a brief explanation.

(a) List all of the primitive elements modulo 13.

Solution. Since it can easily be shown that 2 is a primitive root mod 13, and has order $13-1=12$, the primitive roots are therefore $2^1, 2^5, 2^7$, and 2^{11}, which are $\boxed{\mathbf{2, 6, 7, 11}}$.

(b) Are there any solutions to the congruence $x^4 \equiv 2 \pmod{17}$?

Solution. There are solutions if and only if $2^{\frac{16}{(4,16)}} \equiv 1 \pmod{17}$. But $2^4 \equiv 16 \pmod{17}$, so there are $\boxed{\textbf{No solutions}}$.

(c) How many solutions are there to the congruence $x^8 \equiv 1 \pmod{19}$?

Solution. Since $(8, 18) = 2$, there are $\boxed{\textbf{2 solutions}}$.

(d) Determine whether $x^2 \equiv 35 \pmod{79}$ is solvable.

Solution. Using generalized quadratic reciprocity, calculate

$$\left(\frac{35}{79}\right) = -\left(\frac{79}{35}\right) = -\left(\frac{9}{35}\right) = -\left(\frac{3}{79}\right)^2 = -1.$$

Thus 35 is a quadratic nonresidue modulo 79, and there are $\boxed{\textbf{No solutions}}$.

(e) If n is odd, evaluate the Jacobi symbol $\left(\frac{n^3}{n-2}\right)$.

Solution. It's easiest to begin by removing the square factor (note that $(n, n-2) = 1$)

$$\left(\frac{n^3}{n-2}\right) = \left(\frac{n}{n-2}\right) = \left(\frac{2}{n-2}\right) = \boxed{\begin{cases} \mathbf{1} & \text{if } \boldsymbol{n \equiv 1, 3} \pmod{\mathbf{8}} \\ \mathbf{-1} & \text{if } \boldsymbol{n \equiv 5, 7} \pmod{\mathbf{8}}. \end{cases}}$$

(f) If $p \equiv 7 \pmod{12}$, calculate $\left(\frac{-3}{p}\right)$.

Solution. Using quadratic reciprocity,

$$\left(\frac{-3}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{3}{p}\right) = (-1)\cdot -1\left(\frac{p}{3}\right) = \left(\frac{1}{3}\right) = \boxed{\mathbf{1}}.$$

(g) Calculate the continued fraction expansion of $\frac{78}{31}$.

Solution.

$$\frac{78}{31} = 2 + \frac{16}{31} = 2 + \frac{1}{\frac{31}{16}} = 2 + \frac{1}{1 + \frac{15}{16}}$$
$$= 2 + \frac{1}{1 + \frac{1}{\frac{16}{15}}} = \boxed{\mathbf{2 + \cfrac{1}{1 + \cfrac{1}{1 + \cfrac{1}{15}}}}}.$$

Problem 2. (*15 pts: 5+5+5*) **(a)** Find the solutions to $x^3 + 2x^2 - 3 \equiv 0 \pmod 7$ and determine whether they are singular or nonsingular.

Solution. Write $f(x) = x^3 + 2x^2 - 3$, and then $f'(x) = 3x^2 + 4x$. Checking all values of x gives the roots 1 and 3. Furthermore, $f'(1) = 7 \equiv 0 \pmod 7$ and $f'(3) = 39 \not\equiv 0 \pmod 7$. Thus the roots are $\boxed{\boldsymbol{x = 1;\ \text{singular}}}$ and $\boxed{\boldsymbol{x = 3;\ \text{nonsingular}}}$.

(b) Given that 2 is a primitive root modulo 29 and that $3^7 \equiv 12 \pmod{29}$, find all solutions to $x^7 \equiv 12 \pmod{29}$.

Solution. The solutions all have the form $3 \cdot 2^{4k}$ for $0 \leq k \leq 6$. Specifically, they are (in order of k) $\boxed{\mathbf{3, 19, 14, 21, 17, 11, 2}}$.

(c) Given that 22 is a primitive root modulo 25, find a primitive root modulo 250.

Solution. Since 22 is primitive modulo 5^2, it is automatically a primitive root modulo 5^3. Finally, a primitive root modulo $250 = 2 \cdot 5^3$ must be odd, which is accomplished by adding 125 to 22, giving $\boxed{\mathbf{147}}$.

Problem 3. (*20 pts: 5+10+5*) Suppose that $p \equiv 1 \pmod 4$ is prime. **(a)** Show that a is a quadratic residue modulo p if and only if $p - a$ is a quadratic residue modulo p.

Solution. Using Legendre symbols,

$$\left(\frac{p-a}{p}\right) = \left(\frac{-a}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{a}{p}\right) = 1 \cdot 1,$$

since $p \equiv 1 \pmod 4$ and a is known to be a quadratic residue.

(Bonus) (*3 pts*) Show that a is a quadratic residue modulo p if and only if $\overline{a}$ is.

Solution.

$$\left(\frac{\overline{a}}{p}\right) = \left(\frac{\overline{a}}{p}\right)\left(\frac{a^2}{p}\right) = \left(\frac{a}{p}\right) = 1.$$

(b) Calculate the sum of all of the quadratic residues modulo p (find the sum as an integer – do not reduce it mod p!).

Solution. Since there are an equal number of quadratic residues and nonresiduces, there are exactly $\frac{p-1}{2}$ quadratic residues. Furthermore, these occur in pairs a and $p-a$. There are $\frac{p-1}{4}$ such pairs, so the total sum is $\boxed{\dfrac{\boldsymbol{p(p-1)}}{\mathbf{4}}}$.

(c) Calculate the sum of the quadratic nonresidues modulo p.

Solution. The total sum of residues and nonresidues is $1 + 2 + \cdots + p - 1 = \frac{p(p-1)}{2}$. Thus the sum of the quadratic residues is exactly half the total, and the nonresidues is the other half, and is also equal to $\boxed{\dfrac{\boldsymbol{p(p-1)}}{\mathbf{4}}}$.

Problem 4. (*15 pts: 7+8*) **(a)** Calculate $\left(\dfrac{69}{107}\right)$.

Solution.

$$\left(\frac{69}{107}\right) = \left(\frac{107}{69}\right) = \left(\frac{38}{69}\right) = \left(\frac{2}{69}\right)\left(\frac{19}{69}\right) = -1 \cdot \left(\frac{69}{19}\right)$$
$$= -\left(\frac{12}{19}\right) = -\left(\frac{4}{19}\right)\left(\frac{3}{19}\right) = -1 \cdot 1 \cdot -\left(\frac{19}{3}\right) = \left(\frac{1}{3}\right) = \boxed{\mathbf{1}}\,.$$

(b) Determine whether $3x^2 - 4x + 14 \equiv 0 \pmod{107}$ is solvable.

Solution. Multiply by 3 and then complete the square:

$$\begin{aligned} & 9x^2 - 12x + 42 \equiv 0 \pmod{107} \\ \iff & (3x-2)^2 + 38 \equiv 0 \pmod{107} \\ \iff & (3x-2)^2 \equiv -38 \pmod{107}. \end{aligned}$$

This has solutions if and only if $\left(\frac{-38}{107}\right) = 1$, but $-38 \equiv 69 \pmod{107}$. By part (a), the equation $\boxed{\textbf{is solvable}}$.

Problem 5. (*15 pts: 10+5*) Define the periodic continued fractions $\theta_n := \overline{[1, 2, \ldots, n]}$.
(a) Evaluate θ_1 and θ_2.

Solution. From the book, $\theta_1 = [\,\overline{1}\,] = \boxed{\dfrac{\mathbf{1+\sqrt{5}}}{\mathbf{2}}}$.

For the second, expand the continued fraction and solve.

$$\theta_2 = 1 + \cfrac{1}{2 + \cfrac{1}{\theta_2}} \qquad \Longrightarrow \qquad \theta_2 = 1 + \frac{\theta_2}{2\theta_2 + 1}$$
$$\Longrightarrow \quad \theta_2(2\theta_2 + 1) = 2\theta_2 + 1 + \theta_2 \qquad \Longrightarrow \qquad 2\theta_2^2 - 2\theta_2 - 1 = 0.$$

Now the quadratic formula gives

$$\theta_2 = \frac{2 + \sqrt{4+8}}{4} = \boxed{\frac{\mathbf{1+\sqrt{3}}}{\mathbf{2}}}\,.$$

(b) Prove the following inequalities:

$$\begin{cases} \theta_n < \theta_{n+1} & \text{if n is even,} \\ \theta_n > \theta_{n+1} & \text{if n is odd.} \end{cases}$$

Solution. Note that $\theta_n = [1, 2, \ldots, n, \theta_n]$, whereas $\theta_{n+1} = [1, 2, \ldots, n, n+1, \theta_{n+1}]$. In other words,

$$\begin{aligned} \theta_n &= [1, 2, \ldots, n, x] \qquad \text{and} \qquad \theta_{n+1} = [1, 2, \ldots, n, y], \\ &\text{with} \quad 1 < x < 2 \qquad \text{and} \qquad n+1 < y < n+2. \end{aligned}$$

In particular, $x < y$, and thus the result from the homework gives the claimed inequalities (the result was that if $d < c$, then

$$[a_0, a_1, \ldots, a_n, d] < [a_0, a_1, \ldots, a_n, c]$$

when n is odd, with the opposite inequality for n even).

(Bonus) (*2 pts*) Does $\lim_{n\to\infty} \theta_n$ exist? If so, what is it?

Solution. Yes, the limit is the *non-periodic* continued fraction $\boxed{\mathbf{[1, 2, 3, 4, \ldots]}}$.