Solutions

Math 445

Final Exam

Do any five (5) of the following six (6) problems. All problems have equal weight.

Show all work. How you get your answer is just as important, if not more important, than the answer itself. If you think it, write it!

1. Show that for any integers $k \geq 1$ and $a \geq 2$,
$$k|\phi(a^k - 1)$$
(Hint: What can you say about the order of a mod $m = a^k - 1$?)

$\text{ord}_m(a) =$ smallest n with $a^n \underset{m}{\equiv} 1$ i.e.

$m = a^k - 1 \mid a^n - 1$. $\quad a^k - 1 \mid a^n - 1 \Rightarrow a^k - 1 \leq a^n - 1$

$\Rightarrow k \leq n$.

But $a^k \underset{m}{\equiv} 1$ so $\text{ord}_m(a) = k$.

But in general, $\text{ord}_m(a) \mid \phi(m) = \phi(a^k - 1)$.

So $k \mid \phi(a^k - 1)$.

2. Find the ~~length~~ period **of** the repeating decimal expansion of $\frac{1}{47}$.

length of repeating decimal $= \text{ord}_{47}(10) = n$

$n \mid \phi(47) = 46 = 2\cdot 23 \Rightarrow n = 1, 2, 23, \text{ or } 46$

$10^1 = 10 \underset{47}{\equiv} 10 \Rightarrow n \neq 1$

$10^2 = 100 \underset{47}{\equiv} 94+6 \underset{47}{\equiv} 6 \Rightarrow n \neq 2$

$10^4 \equiv 6^2 \equiv 36$

$10^8 \equiv 36^2 = 1296 \underset{47}{\equiv} 27$

$10^{16} \equiv 27^2 = 729 \underset{47}{\equiv} 24$

$10^{24} = 10^{16}\cdot 10^8 \underset{47}{\equiv} 27\cdot 24 = 648 \underset{47}{\equiv} 37$

so $10^{24} \underset{47}{\not\equiv} 10$ so $10^{23} \underset{47}{\not\equiv} 1$

$\underline{\text{so}}$ $n \neq 23$

$\Rightarrow n = 46$, so

$\text{ord}_{47}(10) = 46$

$$\begin{array}{r} 27 \\ \times\ 24 \\ \hline 108 \\ 54 \\ \hline 648 \end{array} \qquad \begin{array}{r} 36 \\ \times\ 36 \\ \hline 216 \\ 108 \\ \hline 1296 \end{array}$$

$$\begin{array}{r} 13 \\ 47\overline{)648} \\ 47 \\ \hline 178 \\ 141 \\ \hline 37 \end{array} \qquad \begin{array}{r} 27 \\ 47\overline{)1296} \\ 94 \\ \hline 356 \\ 329 \\ \hline 27 \end{array} \qquad \begin{array}{r} 15 \\ 47\overline{)729} \\ 47 \\ \hline 259 \\ 235 \\ \hline 24 \end{array}$$

3. Use continued fractions to find a solution to the Diophantine equation
$$x^2 - 43y^2 = -2$$

$6 < \sqrt{43} < 7$ $\qquad a_0 = 6 \qquad x_0 = \sqrt{43} - 6$

$\dfrac{1}{\sqrt{43}-6} = \dfrac{\sqrt{43}+6}{7}$ $\qquad a_1 = 1 \qquad x_1 = \dfrac{\sqrt{43}-1}{7}$

$\dfrac{\sqrt{43}+1}{6}$ $\qquad a_2 = 1 \qquad x_2 = \dfrac{\sqrt{43}-5}{6}$

$43 - 25 = 18$ $\qquad \dfrac{\sqrt{43}+5}{3}$ $\qquad a_3 = 3 \qquad x_3 = \dfrac{\sqrt{43}-4}{3}$

$43 - 16 = 27$ $\qquad \dfrac{\sqrt{43}+4}{9}$ $\qquad a_4 = 1 \qquad x_4 = \dfrac{\sqrt{43}-5}{9}$

$x_5 = \dfrac{\sqrt{43}-5}{2}$ $\Longleftarrow$

$\dfrac{\sqrt{43}+5}{2}$ $\qquad a_5 = 5 \qquad x_6 = \dfrac{\sqrt{43}-4}{9}$

$\dfrac{\sqrt{43}+5}{9}$ $\qquad a_6 = 1$

a_i			6	1	1	3	1	5	1
h_i	0	1	6	7	13	46	59		
k_i	1	0	1	1	2	7	9		
$h_i^2 - 43k_i^2$			-7	6	-3	9	-2		

$$\boxed{\begin{array}{l} x = 59 \\ y = 9 \end{array} \quad \underline{\text{solves}} \quad x^2 - 43y^2 = -2}$$

4. Show that if $(p, q) = 1$ and the modular equations

$$x^2 + y^2 \equiv 3 \pmod{p} \quad \text{and} \quad u^2 + v^2 \equiv 3 \pmod{q}$$

have solutions, then the equation

$$r^2 + s^2 \equiv 3 \pmod{pq}$$

has a solution.

(Hint: By adding multiples of p and q (respectively), show that you can arrange solutions with $x = u, y = v$.)

Can change x, y mod p without changing x^2+y^2 mod p $\left(x \underset{p}{\equiv} x' \Rightarrow x^2 \underset{p}{\equiv} x'^2, \text{etc.} \right)$

So $(x+p\alpha)^2 + (y+p\beta)^2 \underset{p}{\equiv} 3$.

Also, $(u+q\gamma)^2 + (v+q\delta)^2 \underset{p}{\equiv} 3$.

Want $x+p\alpha = u+q\gamma \qquad y+p\beta = v+q\delta$, i.e.

$x-u = p(-\alpha)+q(\gamma) \qquad y-v = p(-\beta)+q(\delta)$.

But $(p,q) = 1 \Rightarrow \exists\ \alpha_0, \gamma_0$ so that $p\alpha_0 + q\gamma_0 = 1$ so set

$-\alpha = (x-u)\alpha_0$,

$\gamma = (x-u)\gamma_0$

$-\beta = (y-v)\alpha_0$

$\delta = (y-v)\gamma_0$.

Then $x+p\alpha = A = u+q\gamma$

$y+p\beta = B = v+q\delta$, so

$A^2+B^2 \underset{p}{\equiv} 3$, $A^2+B^2 \underset{q}{\equiv} 3$ i.e.,

$p, q \mid (A^2+B^2-3)$.

But then $(p,q)=1 \Rightarrow pq \mid A^2+B^2-3$, i.e.

$A^2+B^2 \underset{pq}{\equiv} 3$. So the eqn has a solution.

5. Show that if $n \equiv 3 \pmod 4$, then the Diophantine equation

$$x^2 - ny^2 = -1$$

has no solution.

x	x^2
0	0
1	1
2	0
3	1

Look at the equation mod 4.

Want $x^2 - 3y^2 \underset{4}{\equiv} -1 \underset{4}{\equiv} 3$, i.e. $x^2 \underset{4}{\equiv} 3(y^2+1)$

If $y \underset{4}{\equiv} 1$ or 3, then $y^2 \underset{4}{\equiv} 1$ so want $x^2 \underset{4}{\equiv} 3(1+1) = 6 \underset{4}{\equiv} 2$, which is impossible.

If $y \underset{4}{\equiv} 0$ or 2, then $y^2 \underset{4}{\equiv} 0$, so want $x^2 \underset{4}{\equiv} 3(0+1) = 3$, which is impossible.

So $x^2 - 3y^2 \underset{4}{\equiv} x^2 - ny^2 \underset{4}{\equiv} -1$ has no solutions.

So $x^2 - ny^2 = -1$ has no solutions.

Or: $n \underset{4}{\equiv} 3 \Rightarrow n$ has a prime factor $p \underset{4}{\equiv} 3$

(o/w all factors are $\underset{4}{\equiv} 1$, $\Rightarrow n \underset{4}{\equiv} 1$)

Look at the equation mod p.

$$x^2 - ny^2 \underset{p}{\equiv} x^2 \underset{p}{\equiv} -1$$

This has a solution (by Euler's criterion) $\Longleftrightarrow$ $(-1)^{\frac{p-1}{2}} \underset{p}{\equiv} 1$. But $p = 4k+3$, so $\frac{p-1}{2} = \frac{4k+2}{2} = 2k+1$

So $(-1)^{\frac{p-1}{2}} = (-1)^{2k+1} = -1 \underset{p}{\equiv} 1 \Rightarrow p \mid 1-(-1) = 2$

$\Rightarrow p = 1$ or 2 contrad. So $x^2 - ny^2 \underset{p}{\equiv} -1$ has no solution so $x^2 - ny^2 = -1$ has no solution.

6. Find the sum of the points $A = (1, 5)$ and $B = (3, 7)$ on the elliptic curve defined by the function

$$f(x, y) = y^2 - (x^3 - x + 25)$$

where $\underline{0}$ is chosen to be $\underline{0} = (0, -5)$.

$(1,5)$, $(3,7)$ $\qquad \frac{7-5}{3-1} = 1 = \text{slope}$

$y = 5 + 1(x-1) = x+4$. Plug in!

$(x+4)^2 - (x^3 - x + 25) = 0$

$= x^2 + 8x + 16 - x^3 + x - 25 = -(x^3 - x^2 - 9x + 9)$

$= -(x-1)(x^2-9) = -(x-1)(x-3)(x+3)$

$\Rightarrow x = 1, 3, \underline{\underline{-3}}$ $\qquad y = (-3)+4 = 1$ $\qquad$ so

$AB = (-3, 1)$

$A+B = \underline{0}(AB)$, $\underline{0} = (0,-5)$ $\qquad \frac{-5-1}{0-(-3)} = \frac{-6}{3} = -2$

$y = -5 + (-2)(x-0) = -2x - 5$ $\quad$ Plug in!

$0 = (-2x-5)^2 - (x^3 - x + 25)$

$= 4x^2 + 20x + 25 - x^3 + x - 25$

$= -(x^3 - 4x^2 - 21x) = -x(x+3)(x-7)$

$\Rightarrow x = 0, -3, \underline{\underline{7}}$

$\hookrightarrow y = -2(7) - 5 = -19$

so $\boxed{A+B = (7, -19)}$