M E T U
Department of Mathematics

	Elementary Number Theory II Midterm 1	
Code : *Math 366* Acad. Year : *2018-2019* Semester : *Spring* Instructor : *Tolga Karayayla* Date : *02.04.2019* Time : *17.40* Duration : *120 minutes*	Last Name : First Name : Student ID : Department : Signature : 7 Questions on 4 Pages SHOW DETAILED WORK!	

1	2	3	4	5	6	7		

1. (15 pts.) Find all solutions $(x, y, z) \in \mathbb{Z}^3$ of the equation $2x^2 + 3y^2 = 8z^2$.

$z=0 \Rightarrow \boxed{(x,y,z)=(0,0,0)}$ Assume $\boxed{z \neq 0}$, then $2\left(\frac{x}{z}\right)^2 + 3\left(\frac{y}{z}\right)^2 = 8$

$2A^2 + 3B^2 = 8$, $A = \frac{x}{z}, B = \frac{y}{z}$

$(A_0, B_0) = (-2, 0)$ is a rational point on the conic $2A^2+3B^2=8$.

Let L be the line in the AB-plane through $(A,B)=(-2,0)$ with slope $r \in \mathbb{Q}$.

$L: B-0 = r(A-(-2))$, $B = r(A+2)$

$2A^2+3B^2=8 \Leftrightarrow 2A^2+3(r^2(A+2)^2)-8=0$

$2(A^2-4)+3r^2(A+2)^2=0$

$(A+2)\cdot\left[2(A-2)+3r^2(A+2)\right]=0$

$\underbrace{A+2=0}_{}$ $\vee$ $2(A-2)+3r^2(A+2)=0$

gives $(A,B)=(-2,0)$ $\boxed{A = \frac{4-6r^2}{2+3r^2}} \Rightarrow B = r(A+2)$ $\boxed{B = \frac{8r}{2+3r^2}}$

$(A,B) = \left(\frac{4-6r^2}{2+3r^2}, \frac{8r}{2+3r^2}\right)$ is the second intersection of L with the conic $2A^2+3B^2=8$

This parametrizes all rational points on the conic, except for $(-2,0)$

$r = \frac{a}{b} \Rightarrow (A,B) = \left(\frac{4b^2-6a^2}{2b^2+3a^2}, \frac{8ab}{2b^2+3a^2}\right)$ (where $\boxed{r = \frac{a}{b} \in \mathbb{Q}}$) $a,b \in \mathbb{Z}, b \neq 0$.

$$\left.\begin{aligned} \frac{x}{z} &= \frac{4b^2-6a^2}{2b^2+3a^2} \\ \frac{y}{z} &= \frac{8ab}{2b^2+3a^2} \end{aligned}\right\} \Rightarrow (x,y,z) = k\cdot(4b^2-6a^2, 8ab, 2b^2+3a^2)$$ where $a,b \in \mathbb{Z}, b \neq 0$, $k \in \mathbb{Q}$ such that $(x,y,z) \in \mathbb{Z}^3$.

((x,y,z) is proportional to $(4b^2-6a^2, 8ab, 2b^2+3a^2)$ where $a,b \in \mathbb{Z}, b \neq 0$.

So, $(x,y,z)=(0,0,0)$, or $(x,y,z)=(-2k,0,k)$ $k \in \mathbb{Z}$ or

2. (14 pts.) Find all solutions $(x, y, z) \in \mathbb{Z}^3$ of the linear Diophantine equation $24x + 14y + 63z = 1$.

$d = \gcd(24,14,63) = \gcd(\gcd(24,14),63) = \gcd(2,63) = 1$ and $1 \mid 1$ $(d \mid 1)$, hence there is a solution.

$\gcd(24,14) = 2 \Rightarrow \boxed{24x + 14y = 2k}$ for some $k \in \mathbb{Z}$

$24x+14y+63z = 1 \Leftrightarrow 2k + 63z = 1$ $\quad (k,z) = (-31,1)$ is a solution. $\gcd(2,63)=1$.

Then, $\boxed{\begin{array}{l} k = -31 + 63t \\ z = 1 - 2t \end{array} \text{ for } t \in \mathbb{Z}}$

$2k = 24x + 14y = 2\cdot(-31+63t) \Leftrightarrow 12x + 7y = -31 + 63t$

$\gcd(12,7) = 1$

$12 = 7\cdot 1 + 5$

$7 = 5 \cdot 1 + 2$

$5 = 2\cdot 2 + 1$

$2 = 1 \cdot 2 + 0$

$1 = 5 - 2\cdot 2$

$= 5 - 2(7-5)$

$= 3\cdot 5 - 2\cdot 7$

$= 3\cdot(12-7) - 2\cdot 7$

$= 3\cdot 12 - 5\cdot 7$

$(x,y) = (3,-5)$ is a sol. of $12x + 7y = 1$

$12\cdot 3 + 7(-5) = 1$

$12(3\cdot(-31+63t)) + 7(-5(-31+63t)) = -31+63t$

Then $\boxed{\begin{array}{l} x = -93 + 189t + 7u \\ y = 155 - 315t - 12u \\ z = 1 - 2t \end{array}}$ for $t, u \in \mathbb{Z}$

3. (2×7 pts.) For each integer n below, express n as a sum of two squares if it is possible. If not, express n as a sum of four squares:

$\boxed{\begin{array}{l} (a^2+b^2)\cdot(c^2+d^2) \\ = (ac-bd)^2 + (ad+bc)^2 \end{array}}$

a) $n = 2^3 \cdot 7^2 \cdot 29 \cdot 73 = (2\cdot 7)^2 \cdot 2 \cdot 29 \cdot 73 = 14^2 \cdot (1^2+1^2)(5^2+2^2)\cdot(8^2+3^2)$

$= 14^2\cdot(1^2+1^2)[(5\cdot 8 - 2\cdot 3)^2 + (5\cdot 3 + 8\cdot 2)^2]$

$= 14^2 \cdot (1^2+1^2)\cdot(34^2 + 31^2)$

$= 14^2[(1\cdot 34 - 1\cdot 31)^2 + (1\cdot 31 + 1\cdot 34)^2]$

$= 14^2\cdot(3^2 + 65^2) = (14\cdot 3)^2 + (14\cdot 65)^2$

$= 42^2 + 910^2$

b) $n = 13 \cdot 43$ $\quad 13 \equiv 1 \pmod 4$ $\quad 43 \equiv 3 \pmod 4$ $\quad$ power of 43 in the prime factorization is 1 (odd), then n is not a sum of two squares.

$n = 13\cdot(41+2)$

$= 13\cdot 41 + 13\cdot 2$

$= (3^2+2^2)\cdot(5^2+4^2) + (3^2+2^2)(1^2+1^2)$

$= [(3\cdot 5 - 2\cdot 4)^2 + (3\cdot 4 + 2\cdot 5)^2] + [(3\cdot 1 - 2\cdot 1)^2 + (3\cdot 1 + 2\cdot 1)^2]$

$= 7^2 + 22^2 + 1^2 + 5^2$

4. (14 pts.) Find all $(x, y, z) \in \mathbb{Z}^3$ such that $x > 0, y > 0, z > 0$, $x^2 + y^2 = z^2$ and $x + z = 150$.

$(x,y,z) = (kx_0, ky_0, kz_0)$ or $(x,y,z) = (ky_0, kx_0, kz_0)$ where $k \in \mathbb{Z}$ and (x_0, y_0, z_0) is a primitive Pythagorean triple with $x_0, y_0, z_0 \in \mathbb{Z}^+$.

$x_0 = 2st$ $\qquad$ $\gcd(s,t) = 1$

$y_0 = s^2 - t^2$ where $s > t > 0$

$z_0 = s^2 + t^2$ $\qquad$ $s \not\equiv t \pmod 2$

case 1: $x = kx_0$, $z = kz_0$

$150 = x + z = k2st + k(s^2+t^2)$

$150 = k(s^2 + 2st + t^2) = k \cdot (s+t)^2$

$2 \cdot 3 \cdot 5^2 = k \cdot (s+t)^2 \Rightarrow \boxed{k = 6, s+t = 5}$

$s + t = 5 \Rightarrow (s,t) = (4,1)$ or $(s,t) = (3,2)$

$\boxed{(x,y,z) = (48, 90, 102) \text{ or } (x,y,z) = (72, 30, 78)}$

case 2: $x = ky_0$, $z = kz_0$

$x + z = 150 = k(s^2 - t^2) + k(s^2 + t^2)$

$150 = k \cdot 2s^2$

$2 \cdot 3 \cdot 5^2 = k \cdot 2 \cdot 5^2 \Rightarrow \boxed{k = 3, s = 5}$

$s = 5 \Rightarrow t = 4$ or $t = 2$

$(s,t) = (5,4) \Rightarrow (x,y,z) = (27, 120, 123)$

$(s,t) = (5,2) \Rightarrow (x,y,z) = (63, 60, 87)$

5. (14 pts.) Let p and q be two distinct primes such that $p \equiv q \equiv 1 \pmod 4$. Show that pq can be expressed as a sum of two squares in at least two distinct ways (that is, $pq = x^2 + y^2 = s^2 + t^2$ f0r positive integers x, y, s, t such that $(x,y) \neq (s,t)$ and $(x,y) \neq (t,s)$).

$p \equiv q \equiv 1 \pmod 4 \Rightarrow p$ and q are sums of two squares.

$p = a^2 + b^2$ $\quad$ p prime $\Rightarrow a \neq 0, b \neq 0$, and $\gcd(a,b) = 1$ $\quad$ w.l.o.g. $a > 0, b > 0$

$q = c^2 + d^2$ $\quad$ q prime $\Rightarrow c \neq 0, d \neq 0$, $\gcd(c,d) = 1$ $\quad$ $c > 0, d > 0$

$p \cdot q = (a^2 + b^2) \cdot (c^2 + d^2) = (ac - bd)^2 + (ad + bc)^2 = x^2 + y^2$ where $x = |ac - bd|$

$= (ac + bd)^2 + (ad - bc)^2 = s^2 + t^2$

$y = ad + bc$

$s = ac + bd$

$t = |ad - bc|$

$x, y, s, t > 0$

$\Big(x = 0 \Rightarrow pq = y^2$ contradiction (p, q distinct primes) $\Big)$

similarly $y \neq 0, s \neq 0, t \neq 0$.

To show $(x,y) \neq (s,t)$ and $(x,y) \neq (t,s)$, it suffices to show $y \neq t$ and $y \neq s$.

$y = t \Rightarrow \begin{cases} ad + bc = ad - bc \Rightarrow 2bc = 0, b = 0 \vee c = 0, \text{contradicting } b > 0, c > 0 \\ \text{or } ad + bc = -ad + bc \Rightarrow 2ad = 0, \text{contradicting } a > 0, d > 0. \end{cases}$

$y = s \Rightarrow ad + bc = ac + bd$

$a(d - c) = b(d - c)$

$(a - b)(d - c) = 0 \Leftrightarrow a = b \vee d = c$

$p = 2a^2$ (contradicting p is an odd prime)

$q = c^2 + d^2$, $q = 2c^2$ (contradicting q is an odd prime).

6. (14 pts.) For the elliptic curve C given by the equation $y^2 = x^3 - 2x + 1$, find all rational points of finite order on C (Discriminant of $x^3 + bx + c$ is $D = -4b^3 - 27c^2$).

$D = -4(-2)^3 - 27\cdot 1^2 = 5$

Let $(x,y) \in C$ be a rational point of finite order on C. Then by Nagell-Lutz Theorem $x,y \in \mathbb{Z}$, and $y=0$ or $y \mid D = 5$

$y=0 \Rightarrow x^3 - 2x + 1 = 0 \Rightarrow x = 1$ $\quad (x,y) = (1,0) = P$ (a point of order 2 since $-P = (1,-0) = (1,0)$, $-P = P$, $2P = O$)

$y \mid D = 5 \Rightarrow y \in \{\mp 1, \mp 5\}$.

$y = \mp 1 \Rightarrow 1 = x^3 - 2x + 1 \Rightarrow x(x^2-2) = 0 \Rightarrow x = 0$ (since $x \in \mathbb{Z}$)

$(x,y) = (0, \mp 1)$. $\boxed{R = (0,1),\ -R = (0,-1)}$

$y = \mp 5 \Rightarrow 25 = x^3 - 2x + 1 \Rightarrow 0 = x^3 - 2x - 24 \to x = \frac{a}{b} \in \mathbb{Q}$ is a root $\Rightarrow a \mid -24$, $b \mid 1$

so $x \in \{\mp 24, \mp 12, \mp 8, \mp 6, \mp 3, \mp 2, \mp 1\}$

- None of those 14 values is a root.

$y = \mp 5 \Rightarrow$ no $(x, \mp 5)$ with $x \in \mathbb{Z}$ is on C.

order of $P = 2$, order of R = order of $(-R)$

To find order of R:

$R + R = (x_2, y_2) \Rightarrow 2R = R + R = (x_3, -y_3)$

L: Tangent line to C at $R = (0,1)$, $L: y = \lambda x + v$ $\quad \lambda = \frac{f'(0)}{2\cdot 1} = \left.\frac{3x^2-2}{2y}\right|_{(x,y)=(0,1)} = -1$

$1 = \lambda\cdot 0 + v \Rightarrow \boxed{v = 1}$ $\quad L: y = -x + 1$

$x_3 = \lambda^2 - a - 2\cdot x_1 = (-1)^2 - 0 - 2\cdot 0 = 1$, $y_3 = \lambda x_3 + v = -1\cdot 1 + 1 = 0$

Thus, $2R = (x_3, -y_3) = (1, 0) = P$

$2R = P$ has order $2 \Rightarrow R$ has order 4. Then $-R$ also has order 4.

Rational Points of finite order on C are $\{O, P, R, -R\}$ O: identity on C, point at ∞ (Note that $\mathrm{Tors}(C(\mathbb{Q})) \cong \mathbb{Z}/4\mathbb{Z}$)

7. (2 × 7 pts.) a) Show that $\frac{1}{x^4} + \frac{1}{y^4} = \frac{1}{z^4}$ has no solution in integers.

If $\frac{1}{x^4} + \frac{1}{y^4} = \frac{1}{z^4}$, then $x^4y^4z^4\left(\frac{1}{x^4} + \frac{1}{y^4}\right) = x^4y^4z^4 \cdot \frac{1}{z^4}$

$y^4z^4 + x^4z^4 = x^4y^4$

$(yz)^4 + (xz)^4 = (xy)^4$

$a^4 + b^4 = c^4$ with $a,b,c \in \mathbb{Z}$, contradiction.

$(a = yz, b = xz, c = xy)$

This eq. has no sol. unless one of all of a,b,c are 0. but this implies at least one of x,y,z is 0, but then one of $\frac{1}{x}, \frac{1}{y}, \frac{1}{z}$ is not defined

b) Show that any $n \in \mathbb{Z}$ can be written as $n = a^2 + b^2 - c^2$ for some integers a, b and c.

$x \not\equiv 2 \pmod 4 \Rightarrow x = k^2 - m^2$ for $k, m \in \mathbb{Z}$.

Let $n \in \mathbb{Z}$, $n \equiv 1 \pmod 4$ or $n \equiv 3 \pmod 4$ or $n \equiv 0 \pmod 4$ $\Rightarrow n - (2)^2 \not\equiv 2 \pmod 4$

Hence $n - (2)^2 = k^2 - m^2$

$n = k^2 + 2^2 - m^2$, $k, m \in \mathbb{Z}$

$n \equiv 2 \pmod 4 \Rightarrow n^2 - 1^2 \not\equiv 2 \pmod 4$

Hence

$n^2 - 1^2 = k^2 - m^2$

$n = k^2 + 1^2 - m^2$ for $k, m \in \mathbb{Z}$.