M E T U
Mathematics Department

Math 366	Elementary Number Theory II	Spring 2017	MIDTERM 1

Küçüksakallı **March 30, 2017** **17:40 – 19:40**	Name : Last Name :	Student Number : Signature :

P.1 / 25	P.2 / 25	P.3 / 25	P.4 / 25	**SHOW YOUR ORGANIZED WORK**	**Total** / **100**
				GOOD LUCK!	

Q.1) Let (x, y, z) be a Pythagorean triple. The aim of this question is to show that $60|xyz$ by the following steps:

a) Show that $3|xyz$.

Note that switching x and y do not change the product xyz. Without losing of generality, we can assume that a Pythagorean triple is of the form

$$[x, y, z] = \left[\pm d(a^2 - b^2), \pm d(2ab), \pm d(a^2 + b^2)\right]$$

for some $a, b \in \mathbb{Z}$ with $a > b > 0$, $\gcd(a, b) = 1$ and $a + b \equiv 1 \pmod 2$.

If $3|a$ or $3|b$ then we are done. Because, in such a case $3|y$ and therefore $3|xyz$. Otherwise $a^2 \equiv b^2 \equiv 1 \pmod 3$. In that case, $3|x$ and therefore $3|xyz$.

b) Show that $4|xyz$.

Either a or b is even. As a result y must be divisible by 4. As a result the product xyz is divisible by 4.

c) Show that $5|xyz$.

If $5|a$ or $5|b$ then we are done. Because, in such a case $5|y$ and therefore $5|xyz$. Otherwise a^2 and b^2 are congreunt to 1 or 4 modulo 5. If a^2 and b^2 are congruent to the same number modulo 5, then x is divisible by 5. If a^2 and b^2 are congruent to different numbers modulo 5, then z is divisible by 5. In either case $5|xyz$.

Q.2) Let c be a positive integer and let $E : y^2 = x^3 + 4c^4x$.

a) Verify that $P = (2c^2, 4c^3)$ is an element of $E(\mathbb{Q})$.

Note that $(4c^3)^2 = 16c^6 = 8c^6 + 8c^6 = (2c^2)^3 + 4c^4(2c^2)$.

b) Write an equation for the tangent line at P.

Implicit differentiation gives $y' = (3x^2 + 4c^4)/(2y)$. As a result the slope m at the point P is

$$m = \frac{3(2c^2)^2 + 4c^4}{2 \cdot 4c^3} = 2c.$$

The tangent line at P is given by $\ell : y = 2c(x - 2c^2) + 4c^3$.

c) Find the order of P.

Note that $(0, 0)$ is a two torsion point of the elliptic curve E. The line ℓ intersects E at $(0, 0)$ and from this we see that $P \oplus P = (0, 0)$. Since $2P$ has order 2, the point P must have order 4.

Q.3) Show that the equation $3x^2 + 4y^2 = 5z^2$ has no solution in positive integers.

Assume to the contrary that the equation has a solution (x, y, z) in positive integers. Without loss of generality, we can assume that $\gcd(x, y, z) = 1$. If $3|z$, then $3|y$ and therefore $3|x$, which is impossible. Thus $z \not\equiv 0 \pmod 3$. Reducing everything modulo 3, we obtain that $y^2 \equiv 2z^2 \equiv 2 \pmod 3$. This is a contradiction.

Q.4) Consider the Diophantine equation $x^2 + 2y^2 = 3z^2$.

a) Show that (c, c, c) is a solution for each integer c.

Note that $c^2 + 2c^2 = 3c^2$.

b) Find all solutions. Verify your formula by giving a few examples.

Suppose that $z \neq 0$. Then the question is equivalent to finding all rational points on the ellipse $a^2 + 2b^2 = 3$ where $a = x/z$ and $b = y/z$.

Consider the line $\ell : b = r(a-1) + 1$ which passes through $(1, 1)$ with rational slope r. The line ℓ intersects the ellipse at a point $P = (P_a, P_b)$ with rational coordinates. Moreover any line which passes through a rational point and $(1, 1)$ would be of this form.

Putting $b = r(a-1) + 1$ in the equation $a^2 + 2b^2 - 3 = 0$, we get

$$a^2 + 2(r^2(a-1)^2 + 2r(a-1) + 1) - 3 = (a-1)[(2r^2+1)a + (-2r^2 + 4r + 1)] = 0.$$

It follows that

$$P_a = \frac{2r^2 - 4r - 1}{2r^2 + 1} \qquad \text{and} \qquad P_b = r(P_a - 1) + 1 = \frac{-2r^2 - 2r + 1}{2r^2 + 1}.$$

Putting $r = m/n$, we find all solutions $[x, y, z]$ to the Diophantine equation $x^2 + 2y^2 = 3z^2$

$$[x, y, z] = \left[\pm d(2m^2 - 4nm - n^2), \pm d(-2m^2 - 2nm + n^2), \pm d(2m^2 + n^2)\right]$$

for some integers m, n and d. For example if $m = 2, n = 1$ and $d = 1$, we have a solution $(-1, -11, 9)$. Another solution $(5, -23, 19)$ can be found by putting $m = 3, n = 1$ and $d = 1$.

Q.5) Find all solutions of the Diophantine equation $(x^2+2xy+y^2)^2+16 = (y-x+366)^4$.

The equation $a^4+b^4=c^4$ has no solutions in positive integers. The above equation is of this form with $a=x+y, b=2$ and $c=y-x+366$. We must have $x+y=0$ and $y-x+366=\pm 2$. From these two equations, we obtain $-2x+366=\pm 2$. There are only two solutions, namely $(182,-182)$ and $(184,-184)$, to the original equation.

Q.6) a) Represent $m = 99^2 - 2^2$ as a sum of two squares.

It is easy to see that $97 = 9^2+4^2$ and $101 = 10^2+1$. We have $(9+4i)\cdot(10+i) = 86+49i$. Thus $m = 86^2+49^2$.

b) Show that $n = 366^3+2^3$ is not representable as a sum of two squares.

We have $n = (366+2)(366^2-2\cdot 366+2^2)$. Observe that $368 = 2^4\cdot 23$ and

$$366^2 - 2\cdot 366 + 2^2 \equiv (-2)^2 - 2(-2) + 2^2 \equiv 12 \pmod{23}.$$

The square free part of n is divisible by 23 which is a prime of the form $4k+3$. We conclude that n can not be represented as a sum of two squares.