M E T U
Department of Mathematics

<table>
<tr><td colspan="2">Elementary Number Theory II
Midterm 1</td></tr>
<tr><td>Code : Math 366
Acad. Year : 2015
Semester : Spring
Instructor : Küçüksakallı

Date : March 24, 2015
Time : 17:40
Duration : 100 minutes</td><td>Last Name :
Name :
Student No. :
Signature :

6 QUESTIONS ON 4 PAGES
100 TOTAL POINTS</td></tr>
</table>

1	2	3	4	5	6		

1. (12pts) Consider the integers $m = 401, n = 901$ and $k = 1603$.

(a) Express $m \cdot n$ as a sum of two squares.

Solution: We can obtain such a representation by using the identity which convert a product of sums of squares to a sum of squares: $401 \cdot 901 = (20^2 + 1) \cdot (30^2 + 1) = (20 \cdot 30 - 1 \cdot 1)^2 + (20 \cdot 1 + 30 \cdot 1) = 599^2 + 50^2$.

(b) Express $m \cdot k$ as a sum of four squares.

Solution: We have $m = 20^2 + 1$ and $n = 40^2 + 1^2 + 1^2 + 1^2$. Set $\alpha = 20 + i$ and $\beta = 40 + i + j + k$. Using the Hamiltonian product we get $\alpha\beta = 799 + 60i - 19j + 21k$. Therefore we have $401 \cdot 1603 = 799^2 + 60^2 + 19^2 + 21^2$.

2. (12pts) A right triangle with sides of integer length has circumference $2pq$ where p and q are primes such that $p < q$. Find the area of this triangle in terms of p and q.

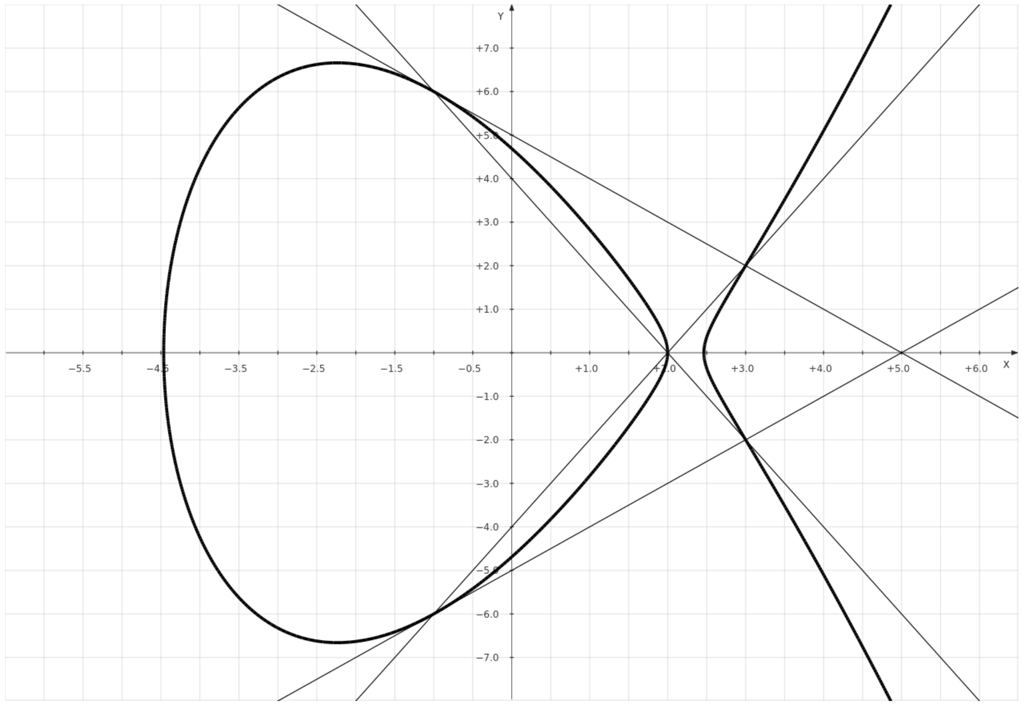
Solution: The sides of the triangle are of lengths $d(a^2 - b^2), d(2ab)$ and $d(a^2 + b^2)$ for some $a > b > 0$ with $\gcd(a, b) = 1$. We are give that the circumference is equal to $2pq$ with $p < q$. On the other hand the circumference is equal to $d(2a^2 + 2ab) = 2ad(a + b)$. In summary

$$ad(a + b) = pq.$$

Since $a > b > 0$, we must have $d = 1, a = p$ and $q = a + b$. It follows that $b = q - p$ and $a^2 - b^2 = p^2 - (q - p)^2$. Moreover we have $2ab = 2p(q - p)$. The area is equal to

$$A = \frac{(a^2 - b^2)(2ab)}{2} = q(2p - q)p(q - p).$$

3. (24pts) The graph of elliptic curve $E : y^2 = x^3 - 15x + 22$ is given below. Consider $P = (-1, 6), Q = (2, 0)$ and $R = (3, 2)$ which are points on E.



(a) Show that $P + P + P = Q$. Show that P is a torsion point. Find the order of P.

Solution: Using implicit differentiation we find that $y' = (3x^2 - 15)/2y$. We have $y' = -1$ at $P(-1, 6)$. The tangent line to E thru P is $\ell : y = -(x + 1) + 6$. Note that ℓ passes thru $R(3, 2) \in E$. Thus $P + P = -R$ where $-R = (3, -2)$. Now we want to compute $P + (P + P) = P + (-R)$. The line passing through P and $-R$ has the equation $y = -2(x+1)+6$. Note that this line intersect E at a third point $Q(2, 0)$. The symmetry along the x-axis leave Q fixed and we have $P + P + P = Q$. Note that $Q + Q = \infty$. It follows that $6P = \infty$. Since the order of P is not equal to 2 or 3, we conclude that the order of P is 6.

(b) Show that $R + R + R = \infty$. Show that $y'' = 0$ at R.

Solution: We can use the fact $R = -2P$ from part (a). It follows that $3R = -6P = \infty$. Now we want to see that y'' vanishes at $R(3, 2)$. We have

$$y'' = \frac{6x \cdot 2y - (3x^2 - 15) \cdot 2y'}{(2y)^2}.$$

Since $y' = 3$ at R, it follows that

$$y'' = \frac{18 \cdot 4 - 12 \cdot 6}{4^2} = 0.$$

4. (16pts) Find all solutions of the Diophantine equation $(x^2+2xy+2y^2-5)^4+1=z^4$.

Solution: The Fermat's equation $a^n+b^n=c^n$ with $n=4$ has only the trivial solutions, i.e. $a=0$ or $b=0$. We must have

$$x^2+2xy+2y^2-5=(x+y)^2+y^2-5=0.$$

The equation $(x+y)^2+y^2=5$ has only eight solutions in total; four of them corresponds to $|x+y|=2, |y|=1$ and the other four corresponds to $|x+y|=1, |y|=2$. Moreover z may be either 1 or -1. Therefore there are sixteen solutions in total.

5. (12pts) If p and q are primes of the form $4k+1$, then show that $n=p\cdot q$ can be written as a sum of two squares in at least two different ways (aside from the order and signs of summands).

Solution: There exist integers $a>b>0$ and $c>d>0$ such that $p=a^2+b^2$ and $q=c^2+d^2$. We have the following equalities

$$\begin{aligned} pq &= (ac-bd)^2+(ad+bc)^2 \\ &= (ad-bc)^2+(ac+bd)^2. \end{aligned}$$

The choice of a,b,c and d gives that $ac-bd>0$. Without loss of generality, we can assume that $ad-bc\geq 0$. Because otherwise we can switch p and q.

Note that $ac-bd$ and $ac+bd$ are different. In order to finish the proof, it is enough to see that $ac-bd$ and $ad-bc$ are different.

Assume otherwise, and consider the equation $ac-bd=ad-bc$. From here, we get $c(a+b)=d(a+b)$. It follows that $c=d$ and $q=c^2+d^2=2c^2$ gives a contradiction.

6. (24pts) Find all integer solutions of the equation $a^2 + 3b^2 = c^2$. Verify your formula by giving a few examples.

Solution: Suppose that $c \neq 0$. Then the question is equivalent to finding all rational points on the ellipse $x^2 + 3y^2 = 1$ where $x = a/c$ and $y = b/c$.

Consider the line $\ell : y = r(x-1)$ which passes through $(1, 0)$ with rational slope r. The line ℓ intersects the ellipse at a point $P = (P_x, P_y)$ with rational coordinates. Moreover any line which passes through a rational point and $(0, 1)$ would be of this form.

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

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

It follows that

$$P_x = \frac{3r^2 - 1}{3r^2 + 1} \qquad \text{and} \qquad P_y = r(P_x - 1) = \frac{-2r}{3r^2 + 1}.$$

Putting $r = m/n$, we find that all positive solutions to the Diophantine equation $x^2+3y^2 = z^2$ are given by

$$(|d(3m^2 - n^2)|, |d(2mn)|, |d(3m^2 + n^2)|).$$

for some integers m, n and d. For example if $m = 2, n = 1$ and $d = 1$, we have a positive solution $(11, 4, 3)$. Another positive solution $(17, 6, 28)$ can be found by putting $m = 3, n = 1$ and $d = 1$. With possible change of signs, one can obtain all other solutions by this formula.