Math 209-16 Homework 6

Due Date: 5pm, Dec. 20 (Tue), 2022

P1.(2 pts) Let a and b be positive integers with $(a,b)=1$. Let $\mathscr{S}$ denote the set of all integers that may be expressed in the form $ax+by$ where x and y are non-negative integers. Show that $c=ab-a-b$ is not a member of $\mathscr{S}$, but that every integer larger than c is a member of $\mathscr{S}$.

Proof. Assume that $c \in \mathscr{S}$, i.e., $ab-a-b=ax+by$ with x,y non-negative. Then $a(b-1-x)=b(y+1)$, hence $a|(y+1)$ and $b|(b-1-x)$ since $(a,b)=1$. This gives us $y \geqslant a-1$ and $x \geqslant b-1$, and therefore $ab-a-b \geqslant a(b-1)+b(a-1)=2ab-a-b$, which is absurd.

On the other hand, for any integer $d>c$, we may first find integers s,t with $d=as+bt$ since a and b are coprime. Then any integer solution of the equation $d=ax+by$ is of the form $x=s+bk$ and $y=t-ak$ for some $k \in \mathbb{Z}$. Now we choose k so that $0 \leqslant x < b$, then $by=d-ax \geqslant (ab-a-b+1)-a(b-1)=-b+1$ and so $y \geqslant 0$. Thus indeed we obtain a solution such that x,y are both non-negative. $\square$

P2.(2 pts) Let u and v be positive integers whose product uv is a perfect square, and let $g=(u,v)$. Show that there exist positive integers r,s such that $u=gr^2$ and $v=gs^2$.

Proof. Let $u=gu_1, v=gv_1$ with $(u_1,v_1)=1$. Then u_1v_1 is also a perfect square. By Lemma 5.4, u_1,v_1 are both perfect squares, and so $u_1=r^2$, $v_1=s^2$. $\square$

P3.(2 pts) Let x,y,z be positive integers such that $(x,y)=1$ and $x^2+5y^2=z^2$. Show that if x is odd and y is even then there exist integers r and s such that x,y,z are given by the equations of Problem 12. Show that if x is even and y is odd then there exist integers r and s such that $x=\pm(2r^2+2rs-2s^2), y=2rs+s^2, z=2r^2+2rs+3s^2$.

Proof. First assertion: From $(x,y)=1$ we see that $(x,z)=1$. Since x is odd and y is even, z is odd. The equation becomes $(\frac{z+x}{2})(\frac{z-x}{2})=5(\frac{y}{2})^2$, and we have $(\frac{z+x}{2},\frac{z-x}{2})=1$ (See the proof between Lemma 5.4 and Theorem 5.5). Write $\frac{z+x}{2}=5s^2, \frac{z-x}{2}=r^2$ or $\frac{z+x}{2}=r^2, \frac{z-x}{2}=5s^2$, then we get integers r,s such that x,y,z are given by the equations of Problem 12.

Second assertion: Similarly, $(x, z) = 1$. Since x is even and y is odd, z is odd and so $(z + x, z - x) = 1$. Now $5y^2 = (z + x)(z - x)$ gives us $z + x = t^2, z - x = 5s^2$, or $z + x = 5s^2, z - x = t^2$. Moreover, we may write $t = 2r + s$ because both t and s are odd. Putting these together we immediately get the result. $\square$

P4.(2 pts) Using the proof of Theorem 5.5 as a model, show that if x and y are integers for which $x^4 - 2y^2 = 1$, then $x = \pm 1, y = 0$.

Proof. It's clear that $x = \pm 1$ and $y = 0$ give solutions to this equation. Next assume $x \neq \pm 1$. Obviously x should be odd, and $2y^2 = (x^2 + 1)(x + 1)(x - 1)$ tells us y should be even. Say $y = 2y_1$, then $y_1^2 = \frac{x^2+1}{2} \cdot \frac{x+1}{2} \cdot \frac{x-1}{2}$. But $\frac{x+1}{2} = \frac{x-1}{2} + 1$, and $\frac{x^2+1}{2} = \frac{x^2-1}{2} + 1$, so we see that $\frac{x^2+1}{2}$, $\frac{x+1}{2}$, and $\frac{x-1}{2}$ are pairwise coprime. As a result, they must all be perfect squares. In particular, $\frac{x-1}{2}$ and $\frac{x+1}{2}$ are consecutive integers which are both perfect squares, and hence $x = 1$, contradiction. $\square$

P5.(2 pts) Show that if $x^3+2y^3+4z^3 \equiv 6xyz \pmod 7$ then $x \equiv y \equiv z \equiv 0 \pmod 7$. Deduce that the equation $x^3 + 2y^3 + 4z^3 = 6xyz$ has no nontrivial integral solutions.

Proof. First notice that if one of x, y, z is divisible by 7, then so are the other two, due to the fact that $a^3 \equiv \pm 1 \pmod 7$ if $a \not\equiv 0 \pmod 7$. For example, if $x \equiv 0 \pmod 7$, then $y^3 \equiv -2z^3 \pmod 7$, and so $y \equiv z \equiv 0 \pmod 7$. Now if none of x, y, z is divisible by 7, then we multiply the inverse of z and get $u^3 + 2v^3 + 4 \equiv 6uv \pmod 7$ with u, v not divisible by 7 either. At this stage we may just check by hand that the above congruence cannot be fulfilled. Therefore $x^3 + 2y^3 + 4z^3 \equiv 6xyz \pmod 7$ implies $x \equiv y \equiv z \equiv 0 \pmod 7$, and so any nontrivial integral solution to $x^3 + 2y^3 + 4z^3 = 6xyz$ would contribute to a strictly smaller one by dividing x, y, z simultaneously by 7, which would clearly lead to a contradiction. $\square$

P6.(2 pts) Show that there exist no positive integers m and n such that $m^2 + n^2$ and $m^2 - n^2$ are both perfect squares.

Proof. We first claim that the equation $x^4 + y^2 = z^4$ has no nontrivial integral solution. We may assume x, y, z relatively prime, and there are two possibilities:
Case 1: $x^2 = r^2 - s^2$, $y = 2rs$, $z^2 = r^2 + s^2$; or Case 2: $x^2 = 2rs$, $y = r^2 - s^2$, $z^2 = r^2 + s^2$, with r and s coprime and having different parities.

In the first case, we obtain $x^2z^2 = r^4 - s^4$, ending up with a strictly smaller solution of $x^4 + y^2 = z^4$.

In the second case, we have $r = 2r_1^2$, $s = s_1^2$, and moreover $z = t^2 + k^2$, $r = 2tk$, $s = t^2 - k^2$. Hence $tk = r_1^2$ and so $t = t_1^2$, $k = k_1^2$, giving us $s = s_1^2 = t_1^4 - k_1^4$, which is again a strictly smaller solution of $x^4 + y^2 = z^4$.

In any case, we then conclude the proof of this claim by Fermat's infinite descent.

Now assume $m^2 + n^2 = a^2$ and $m^2 - n^2 = b^2$, then $m^4 - n^4 = (ab)^2$, which has no solution in positive integers by the claim above. □

P7.(2 pts) Consider a right triangle the lengths of whose sides are integers. Prove that the area cannot be a perfect square.

Proof. Assume there is a right triangle with side lengths a, b, c satisfying $a^2 + b^2 = c^2$ and $ab = 2m^2$. Then $c^2 + (2m)^2 = (a+b)^2$ and $c^2 - (2m)^2 = (a-b)^2$ would both be perfect squares, contradicting the conclusion in Problem 6. □

P8.(2 pts) Prove that if α is algebraic of degree n, and β is algebraic of degree m, then $\alpha + \beta$ is of degree $\leqslant mn$. Prove a similar result for $\alpha\beta$.

Proof 1. According to the proof of Theorem 9.12 in the textbook, we see that $\alpha + \beta$ satisfies a system of homogeneous linear equations in $\theta_1, \theta_2, \ldots, \theta_r$ where θ_i's are the numbers $\alpha^s\beta^t$ with $s = 0, 1, \ldots, n-1$ and $t = 0, 1, \ldots, m-1$. Since the θ_i's are not all zero, the determinant of coefficients is equal to zero. Therefore, $\alpha + \beta$ satisfies a monic polynomial equation of degree $r = mn$ over $\mathbb{Q}$, and hence the degree of the minimal polynomial of $\alpha + \beta$ is $\leqslant mn$, i.e., $\alpha + \beta$ is of degree $\leqslant mn$. Similarly, we can conclude that $\alpha\beta$ is of degree $\leqslant mn$. □

Proof 2. (Using the field extension) Clearly, we have $[\mathbb{Q}(\alpha) : \mathbb{Q}] = n$, $[\mathbb{Q}(\beta) : \mathbb{Q}] = m$ by assumption. Since the minimal polynomial of β over $\mathbb{Q}(\alpha)$ is a divisor of its minimal polynomial over $\mathbb{Q}$, it should have degree not larger than m. Hence, we have $[\mathbb{Q}(\alpha, \beta) : \mathbb{Q}(\alpha)] \leqslant m$ and so $[\mathbb{Q}(\alpha, \beta) : \mathbb{Q}] = [\mathbb{Q}(\alpha, \beta) : \mathbb{Q}(\alpha)] \cdot [\mathbb{Q}(\alpha) : \mathbb{Q}] \leqslant mn$. In particular, both of the degrees of $\alpha + \beta$ and $\alpha\beta$ in $\mathbb{Q}(\alpha, \beta)$ are $\leqslant mn$. □

P9.(2 pts) For any algebraic number α, define m as the smallest positive rational integer such that $m\alpha$ is an algebraic integer. Prove that if $b\alpha$ is an algebraic integer, where b is a rational integer, then $m|b$.

Proof. By division algorithm, we have $b = qm + r$ where $0 \leqslant r < m$. Then we see that $r\alpha = b\alpha - qm\alpha$ is also an algebraic integer. Now $r = 0$ follows from the minimality of m and hence $m|b$. $\square$

P10.(2 pts) If α and $\beta \neq 0$ are integers in $\mathbb{Q}(\sqrt{m})$, and if $\alpha|\beta$, prove that $\overline{\alpha}|\overline{\beta}$ and $N(\alpha)|N(\beta)$.

Proof. Note that the number x is an integer in $\mathbb{Q}(\sqrt{m})$ if and only if its conjugate $\overline{x}$ is an integer. Since $\alpha|\beta$, there exists an integer γ in $\mathbb{Q}(\sqrt{m})$ such that $\beta = \alpha \cdot \gamma$. Now taking the conjugate (Acting the nontrivial automorphism of $\mathrm{Aut}_{\mathbb{Q}}\mathbb{Q}(\sqrt{m})$ on both sides), we obtain $\overline{\beta} = \overline{\alpha} \cdot \overline{\gamma}$. Since γ is an integer in $\mathbb{Q}(\sqrt{m})$, $\overline{\gamma}$ is also an integer in $\mathbb{Q}(\sqrt{m})$ and hence $\overline{\alpha}|\overline{\beta}$. By Theorem 9.21, we have $N(\beta) = N(\alpha)N(\gamma)$, therefore, $N(\alpha)|N(\beta)$ since $N(\gamma) \in \mathbb{Z}$. $\square$