Problem 1. *The curve*

$$y^2 = x^3 + 8$$

contains the point $(1, -3)$ *and* $(-7/4, 13/8)$*. The line through these two points intersects the curve in exactly one other point. Find it and explain why its coordinates are rational numbers.*

Answer. The equation of the line joigning the 2 points is given by : $\frac{y+3}{x-1} = \frac{13/8+3}{-7/4-1} = -\frac{37}{22}$, so it is $y = -\frac{37}{22}x - \frac{25}{22}$. Plug this into the equation of the curve:

$$x^3 + 8 = (-\frac{37}{22}x - \frac{25}{22})^2.$$

This is a cubic equation $x^3 + ax^2 + bx + c$. Since we know already three roots, we know that there is a third one. Moreover, the sum of the three roots must be $(-a) = (37/22)^2 = 1369/484$.Because of this property we know that the third root α must be a rational number (it's a sum of rational numbers). Thus $1 + (-7/4) + \alpha = 1369/484$.So $\alpha = 1732/484$. Plug this into the equation of the line to find the y coordinate.

Problem 2. *Solve* $x^{39} \equiv 3$ *(mod 13) .*

Answer. By Fermat's theorem, you know that $x^{12} \equiv 1$ modulo 13.Therefore $x^{39} \equiv x^{36}.x^3 \equiv x^3$, and we are reduced to the resolution of $x^3 \equiv 3$ modulo 13. You can do it by hand and realize that there is no solution.

Problem 3. *Find all integers n such that* $\phi(n) = n/6$*.(Remember that* $\phi(n)$ *is the number of integers k such that* $1 \leq k \leq n$ *and* $GCD(k, n) = 1$*).*

Answer. Use the formula we had: $\phi(n) = n.(1 - 1/p_1)\ldots(1 - 1/p_k)$, where the p_i are the prime factors appearing in the decomposition of n. Thus we must have $1/6 = (1 - 1/p_1)\ldots(1 - 1/p_k)$. Because of the denominator 6, both prime factors 2,3 must appear. But then $(1 - 1/2).(1 - 1/3) = 1/2$.And among all the other possible factors $(1 - 1/p_i)$, none of them can produce a denominator multiple of 3, therefore the equation has no solution.

Problem 4. *Let* $d_1, \ldots, d_r$ *be the numbers dividing n, including* 1 *and n. The* t^{th} power sigma function $\sigma_t(n)$ *is equal to the sum of the* t^{th} *powers of the divisors of n,*

$$\sigma_t(n) = d_1^t + \ldots + d_r^t.$$

For example, $\sigma_2(10) = 1^2 + 2^2 + 5^2 + 10^2 = 130$.

1. *Compute the values of* $\sigma_3(10), \sigma_0(18)$.
2. *Show that if* $GCD(m, n) = 1$*, then* $\sigma_t(mn) = \sigma_t(m)\sigma_t(n)$.

Answer. 1. $\sigma_3(10) = 1^3 + 2^3 + 5^3 + 10^3 = 1134, \sigma_0(18) = 1+1+1+1+1+1 = 6$.

2. $GCD(m,n) = 1$, then $\sigma_t(mn) = \sigma_t(m)\sigma_t(n)$.

   When m, n are coprime, we proved in the first midterm that there is a bijection between the set of divisors of mn and the set of ordered pairs (d, d'), where d is a divisor of m, and d' is a divisor of n (the correspondance being given by $(d, d') \mapsto d.d'$). Now if we expand the product $\sigma_t(m)\sigma_t(n)$, we get a sum over all the ordered pairs (d, d') (d divisor of m, d' divisor of n), of the tth power of $(d.d')$. By the remark above, we then get the sum of the tth powers of all the divisors of mn, and this is $\sigma_t(mn)$.

Problem 5. *Suppose that a has a square root in $\mathbb{Z}/p\mathbb{Z}$, for p prime, and suppose further that $p \equiv 5$ (mod 8) .*

Show that one of the values $x = a^{p+3}/8$ or $x = (2a).(4a)^{(p-5)/8}$ is a solution to the congruence $x^2 \equiv a$ (mod p) .

Answer. We know that a has a square root, therefore necessarily one has $a^{(p-1)/2} = 1$. Observe that $p = 8k + 5$ implies $p - 1$ is a multiple of 4. Now there are two cases:

1. First case: $a^{\frac{p-1}{4}} = +1$, but then, by multiplying by a both sides one gets: $a^{\frac{p+3}{4}} = +a$. But since $p + 3$ is a multiple of 8, one can consider $x = a^{\frac{p+3}{8}}$ and this will be a square root of a.

2. Second case: $a^{\frac{p-1}{4}} = -1$.But then $a.x^2 = ((2a).(4a)^{(p-5)/8})^2 = a^2.4^{(p-1)/4}.a^{(p-1)/4} = a^2.(-1).(2^{(p-1)/2})$. In the proof of the quadratic reciprocity, we proved that when $p \equiv 5$ (mod 8) we have $2^{(p-1)/2} = -1$, therefore we have $a.x^2 = a^2$, and then x is a square root of a.

Problem 6. 1. *If N is not a perfect square, find a specific value for K so that the inequality $K/b^2 < |a/b - \sqrt{N}|$ holds for every rational number a/b. The value of K will depend on N but not on a or b.)*

2. *Use the above result to find all rational numbers a/b satisfying $|a/b - \sqrt{7}| \leq 1/b^3$.*

Answer. Consider the quadratic polynomial $f(X) = X^2 - N$. Then on the interval $[0, 2\sqrt{N}]$, one has $|f'(x)| = |2x| \leq 4\sqrt{N}$, so one gets $\frac{1}{b^2} < |f(a/b) - f(\sqrt{N})| \leq 4\sqrt{N}.|\frac{a}{b} - \sqrt{N}|$.Now if a/b is larger than $2\sqrt{N}$, then $|\frac{a}{b} - \sqrt{N}| \geq \sqrt{N}$ which is larger than $1/(4\sqrt{N}.b^2)$, so our lower bound works in every case.

Suppose now that you have, $|a/b - \sqrt{7}| \leq 1/b^3$, then you would deduce $K/b^2 \leq 1/b^3$, and therefore $\frac{1}{4\sqrt{7}} < \frac{1}{b}$, so $b < 4\sqrt{7}$, and then $b < 11$, so $b \leq 10$.Now we can try by hand the possible fractions: we find that the only possible solutions are $a/b = 3/1$, and $a/b = 8/3$.

Problem 7. *Let p be a prime number such that $p \equiv 1$ (mod 4) , and assume that $u^2 \equiv -1$ (mod p) . Write u/p as a continued fraction $[a_0, a_1, \ldots a_n]$, and let i be the largest integer such that $q_i \leq \sqrt{p}$ (remember that the q_i are the denominators of the continued fractions $[a_0, \ldots, a_i]$)*

1. *Show that $|p_i/q_i - u/p| < 1/(q_i\sqrt{p})$ and hence that $|p_i p - uq_i| < \sqrt{p}$.*
2. *Put $x = q_i, y = p_i p - uq_i$. Show that $0 < x^2 + y^2 < 2p$, and that $x^2 + y^2 \equiv 0$ (mod p) .Deduce that $x^2 + y^2 = p$.*

Answer.

1. First, we know from the theory of continued fractions that $|p_i/q_i - u/p| \leq 1/(q_i q_{i+1})$ but this implies the result, because necessarily one has $q_{i+1} > \sqrt{p}$ (by definition of q_i).Multiply by the denominators to get the other identity.
2. One has $0 < x^2 + y^2 < q_i^2 + p \leq 2p$. Now $x^2 + y^2 = q_i^2 + (p_i p - uq_i)^2 \equiv q_i^2(1 + u^2) \equiv 0$ (mod p) .And now the conclusion comes from the fact that p is the only multiple of p strictly between 0 and p.

Problem 8. *Prove that $11 + 2\sqrt{6}$ is a prime in $\mathbb{Q}(\sqrt{6})$.(We recall that a prime in a quadratic number field $\mathbb{Q}(\sqrt{m})$ is an element α that is divisible only by invertible elements, and by elements that are products of α by some invertible element).*

Answer. As seen before, we use the Norm map, where $N(a + b\sqrt{6}) = a^2 - 6b^2$. The invertible elements in $\mathbb{Q}(\sqrt{6})$ are the one with norm equal to ± 1. Since $N(11 + 2\sqrt{6}) = 121 - 6.4 = 97$ is prime, so is $11 + 2\sqrt{6}$ (otherwise one could write $11 + 2\sqrt{6}$ as a product $(a + b\sqrt{6}).(c + d\sqrt{6})$ with norms different from ± 1).