

**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.

**Problem 2.** Solve  $x^{39} \equiv 3 \pmod{13}$ .

**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  $\text{GCD}(k, n) = 1$ ).

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

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

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  $\text{GCD}(m, n) = 1$ , then  $\sigma_t(mn) = \sigma_t(m)\sigma_t(n)$ .

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

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

**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  $|a/b - \sqrt{7}| \leq 1/b^3$ .

**Problem 7.** Let  $p$  be a prime number such that  $p \equiv 1 \pmod{4}$ , and assume that  $u^2 \equiv -1 \pmod{p}$ . Write  $u/p$  as a continued fraction  $[a_0, a_1, \dots, a_n]$ , 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  $[a_0, \dots, a_i]$ )

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

**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  $\alpha$  that is divisible only by invertible elements, and by elements that are products of  $\alpha$  by some invertible element).