Solutions for final exam

Lennart Meier

November 25, 2019

Problem 1. *Decide for* 127 *and* $2^{12} + 1 = 4097$ *whether they are prime.*

The primes below $\sqrt{127}$ are $2, 3, 5, 7$ and 11 and 127 is not divisible by any of these.

$2^{12} + 1 = (2^4 + 1)(2^8 - 2^4 + 1) = 17 \cdot 241$ (we discussed this factorization in the context of Fermat primes)

Problem 2 (5 points)**.** *Give an example of a primitive root modulo* 7*.*

A number a is a primitive root modulo 7 if $a^6 \equiv 1 \mod 7$, but a^k is not congruent to 1 for any $1 \leq k \leq 5$. A simple computation shows that 3 is a primitive root.

Problem 3 (24 points)**.** *(a) Show that $\sqrt{11}$ is irrational. (Without citing a theorem from the lecture on October 31.)*

(b) Show that for any $p, q \in \mathbb{N}$, we have $|\sqrt{11} - \frac{p}{q}| > \frac{1}{8q^2}$
(One-point bonus variant: prove it with 7 instead of 8)

(c) Give a fraction $\frac{p}{q}$ with $p, q \in \mathbb{N}$ such that $0 < |\sqrt{11} - \frac{p}{q}| < \frac{1}{3600}$.

a) Either compute the continued fraction expansion of $\sqrt{11}$ and see that it is infinite (as we will do in part c) or just argue as follows: Suppose $\sqrt{11} = \frac{a}{b}$ with a and b relative prime. Then $11b^2 = a^2$. Thus a is divisible by 11 (by Euclid's lemma) and we write it as $11c$. Then $b^2 = 11c^2$ and thus b is also divisible by 11. This is in contradiction with b and a being relatively prime.

b) Suppose (for contradiction) that there are $p, q \in \mathbb{N}$ with $|\sqrt{11} - \frac{p}{q}| \leq \frac{1}{7q^2}$. Multiplying this inequality with $\sqrt{11} + \frac{p}{q}$, we obtain:

$$|11 - \frac{p^2}{q^2}| \leq \frac{\sqrt{11} + \frac{p}{q}}{7q^2}.$$

As $9 < 11 < 11.56$, we have that $3 < \sqrt{11} < 3.4$. Thus, $\frac{p}{q} \leq 3.4 + \frac{1}{7} < 3.6$ and hence $\sqrt{11} + \frac{p}{q} < 7$. Thus we obtain

$$|11 - \frac{p^2}{q^2}| < \frac{7}{7q^2} = \frac{1}{q^2}.$$

Multipliying with q^2, we obtain $|11q^2 - p^2| < 1$. The difference between two natural numbers can only be smaller than 1 if both are equal. Hence $11 = \frac{p^2}{q^2}$ and $\sqrt{11} = \frac{p}{q}$. But $\sqrt{11}$ is irrational (as shown in (a)) and so we obtain a contradiction. [An alternative proof is possible using continued fractions.]

c) We write

$$\begin{aligned}\sqrt{11} &= 3 + (\sqrt{11} - 3)\\ \frac{1}{\sqrt{11}-3} &= \frac{\sqrt{11}+3}{2} = 3 + \frac{\sqrt{11}-3}{2}\\ \frac{2}{\sqrt{11}-3} &= \sqrt{11}+3 = 6 + \sqrt{11} - 3.\end{aligned}$$

This shows that the continued fraction expansion of $\sqrt{11}$ is $[3;\overline{3,6}]$. We can compute the convergents $\frac{p_n}{q_n}$ via the recursive formula $p_{-1} = 1$, $p_0 = a_0$ and $p_n = a_n p_{n-1} + p_{n-2}$ for the p_n and $q_{-1} = 0$, $q_0 = 1$ and $q_n = a_n q_{n-1} + q_{n-2}$ for the q_n. Thus the sequence of p_n starts like this: 3, 10, 63, 199, ... and the sequence of q_n like this: 1, 3, 19, 60,...

We know by a theorem from class that $|\sqrt{11} - \frac{p_n}{q_n}| < \frac{1}{q_n^2}$. Thus, taking $n = 3$, we obtain $|\sqrt{11} - \frac{199}{60}| < \frac{1}{3600}$.

Problem 4 (8 points)**.** *Give two pairs (x, y) of positive integers such that $11y^2 = x^2 + 2x$.*

We add 1 to both sides and substract $11y^2$ to obtain $1 = (x+1)^2 - 11y^2$. This is a Pell's equation. We know that all the solutions $(x + 1, y)$ are of the form (p_n, q_n). Trying the first few, we see that $x + 1 = 10$ and $y = 3$ is the first solution (as $100 - 99 = 1$) and $x + 1 = 199$ and $y = 60$ is the second (as $199^2 - 11 \cdot 60^2 = 1$).

Of course, we don't really have to just naively try these convergents. We know from the continued fraction algorithm above that the denominator of every second α_{2n+1} is 1 for every n. Thus, every pair (p_{2n+1}, q_{2n+1}) is a solution $(x + 1, y)$. (Here we are using that $2n + 1$ is odd.)

Problem 5 (15 points)**.** *Decide for the following two equations whether they have infinitely many solutions (x, y) with $x, y \in \mathbb{Q}$:*

(a) $x^2 + y^2 = 245$

(b) $y^4 = x^4 + 1$

a) The curve cut out by $x^2 + y^2 = 245$ is a circle. Thus, there are infinitely many rational solutions if there is one. Writing $245 = 5 \cdot 49$, we observe that $245 = 7^2 + 14^2$. Thus, we have one solution $(x, y) = (7, 14)$ and hence infinitely many.

b) Let $x = \frac{a}{b}$ and $y = \frac{c}{b}$ be rational numbers with $y^4 = x^4 + 1$ and $a, b, c \in \mathbb{Z}$ (with $b \neq 0$). Multiplying the equation with b^4, we see that it is equivalent to $a^4 + b^4 = c^4$. We have shown in class the special case of Fermat's last theorem that the only solutions of this equation satisfy $a = 0$ or $b = 0$. The latter is already excluded, so we have $a = 0$ and $b = \pm c$. This implies $x = 0$ and $y = \pm 1$. These are only two solutions and not infinitely many.

Problem 6 (8 points)**.** *Show that $y^2 = 29x^2 + 11$ does not have solutions with $x, y \in \mathbb{Z}$.*

Assume that there is a solution (x, y). Considering the equation modulo 29, we see that $y^2 \equiv 11 \mod 29$ and hence the Legendre symbol $\left(\frac{11}{29}\right)$ must be 1.

On the other hand, we compute using quadratic reciprocity:

$$\left(\frac{11}{29}\right) = \left(\frac{29}{11}\right) = \left(\frac{7}{11}\right) = -\left(\frac{11}{7}\right) = -\left(\frac{4}{11}\right) = -1$$

To determine the signs in quadratic reciprocity we use here that $29 \equiv 1 \mod 4$, $11 \equiv 3 \mod 4$ and $7 \equiv 3 \mod 4$. Moreover, the last equality holds because 4 is a square. Thus, we obtain a contradiction and there is no solution.

Problem 7. *Show that there is an integer n between* 219 *and* 2019 *such that n divides $2^n + 2$. (Hint: n can be chosen to be of the form $2pq$ with p and q primes.)*

Let p and q be two different odd primes and $n = 2pq$. By the Chinese remainder theorem, $n|2^n + 2$ is equivalent to

$$\begin{aligned} 2^{2pq} &\equiv -2 \mod 2 \\ 2^{2pq} &\equiv -2 \mod p \\ 2^{2pq} &\equiv -2 \mod q. \end{aligned}$$

The first congruence is automatically fulfilled. Note that $2^{p-1} \equiv 1 \mod p$ and hence

$$2^{2pq} = 2^{2(p-1)q} \cdot 2^{2q} \equiv 2^{2q} \mod p.$$

As 2 is relatively prime to p, we can also divide by 2. Arguing similarly for q, we obtain that the set of congruences above is equivalent to

$$\begin{aligned} 2^{2q-1} &\equiv -1 \mod p \\ 2^{2p-1} &\equiv -1 \mod q \end{aligned}$$

Now it is time for an educated guess. We know that $2^{(p-1)/2} \equiv \left(\frac{2}{p}\right) \mod p$ by Euler's theorem and this is in particular always ± 1. So let's explore the possibility that $\frac{p-1}{2} = 2q - 1$ or, equivalently, that $p = 4q - 1$. As q is odd, this implies that $p \equiv 3 \mod 8$ and hence $\left(\frac{2}{p}\right) = -1$. Thus, $p = 4q - 1$ implies that the first congruence is automatically fulfilled.

Plugging $p = 4q - 1$ into the second congruence yields $2^{8q-3} \equiv -1 \mod q$. As $2^{q-1} \equiv 1 \mod q$, we see that $2^{8q-3} \equiv 2^5 = 32 \mod q$. Thus, the second congruence becomes equivalent with q dividing 33, i.e. $q = 3$ or $q = 11$.

In the case $q = 3$, we obtain $p = 11$ and hence $n = 2pq = 66$. This satisfies $n|2^n + 2$, but $66 < 219$.

In the case $q = 11$, we obtain $p = 43$ (which is prime as it is not divisible by 2, 3 or 5) and hence $n = 2pq = 946$. This satisfies $n|2^n + 2$ and is between 219 and 2019. This solves the problem.

Note that we did not show uniqueness, but this was also not asked for. So we were allowed to use an educated guess to only look at solutions of a specific kind. Restricting the space of solutions makes it often easier to find a solution. (You might have seen this technique before in solving differential equations.)