UNIVERSITY OF CRETE
DEPARTMENT OF MATHEMATICS AND APPLIED MATHEMATICS
NUMBER THEORY - MEM204 (SPRING SEMESTER 2019-20)
INSTRUCTOR: G. KAPETANAKIS

Final exam, September 2020 – Answers

Question 1. i. Show that $30 \mid n^5 - n$, for every $n \in \mathbb{Z}$.

ii. Show that for every $m \in \mathbb{Z}_{>0}$,

$$(2^m + 3^m, 2^{m+1} + 3^{m+1}) = 1.$$

Answer. i. We have that $30 = 2 \cdot 3 \cdot 5$, that is, it suffices to show that 2, 3 and 5 divide $n^5 - n$. In particular, using Fermat's theorem, we have that for every n,

- $n^5 - n \equiv n - n \equiv 0 \pmod 5$,
- $n^5 - n \equiv n^3 \cdot n^2 - n \equiv n \cdot n^2 - n \equiv n^3 - n \equiv n - n \equiv 0 \pmod 3$ and
- $n^5 - n \equiv 0 \pmod 2$, in both cases $n \equiv 0 \pmod 2$ and $n \equiv 1 \pmod 2$.

The result follows.

ii. Assume that $(2^m + 3^m, 2^{m+1} + 3^{m+1}) > 1$. If follows that there exists some prime p, such that $p \mid 2^m + 3^m$ and $p \mid 2^{m+1} + 3^{m+1}$. We take the second relation:

$$p \mid 2^{m+1} + 3^{m+1} = 2 \cdot 2^m + 3 \cdot 3^m = 2 \cdot (2^m + 3^m) + 3^m.$$

Since $p \mid 2^m + 3^m$, the latter yields $p \mid 3^m \overset{p \text{ prime}}{\Longrightarrow} p \mid 3$. Next, we have that

$$p \mid 3 \Rightarrow p \mid 3^m \overset{p \mid 2^m + 3^m}{\Longrightarrow} p \mid 2^m \overset{p \text{ prime}}{\Longrightarrow} p \mid 2.$$

The facts $p \mid 2$ and $p \mid 3$ imply $p \mid 1$, a contradiction. □

Question 2. i. Prove that

$$\sum_{d \mid n} \mu(d)\tau(d) = \begin{cases} 1, & \text{if } n = 1, \\ (-1)^k, & \text{if } n = p_1^{n_1} \cdots p_k^{n_k}. \end{cases}$$

ii. Find the residue of 2020^{2021} divided by 9.

Answer. i. We present two different approaches/answers to this. For the second approach some further knowledge from combinatorics are required.

Number-theoretic approach: We know that both $\mu(x)$ and $\tau(x)$ are multiplicative, hence $\mu(x)\tau(x)$ is multiplicative. It follows that $\sum_{d \mid n} \mu(d)\tau(d)$ is multiplicative as a function of n. Similarly, $f(n) := \begin{cases} 1, & \text{if } n = 1, \\ (-1)^k, & \text{if } n = p_1^{n_1} \cdots p_k^{n_k} \end{cases}$ is clearly multiplicative. It follows that it suffices to prove the desired equality for the case $n = p^r$, where p is a prime and $r \geq 1$.

In this case we have that

$$\sum_{d \mid p^r} \mu(d)\tau(d) = \sum_{i=0}^{r} \mu(p^i)\tau(p^i) = \mu(1)\tau(1) + \mu(p)\tau(p) = 1 - 2 = -1 = f(p^r),$$

since $\mu(p^r) = 0$, for $r \geq 2$, $\mu(1) = \tau(1) = 1$, $\mu(p) = -1$ and $\tau(p) = 2$.

Cobinatorial approach: The case $n = 1$ is trivial. Now, assume that $n \neq 1$, that is, $n = p_1^{n_1} \cdots p_k^{n_k}$. We have that a divisor of n is of the form $d = p_i^{d_1} \cdots p_k^{d_k}$, where $0 \leq d_i \leq n_i$ for all i. Observe that if $d_i > 1$ for some i, then $\mu(d) = 0$, thus, on the sum on the RHS of the equation of interest, only the square-free divisors contribute. It follows that

$$\sum_{d|n} \mu(d)\tau(d) = \sum_{d|p_1\cdots p_k} \mu(d)\tau(d) = \sum_{i=0}^{k} \left(\sum_{1\leq j_1 \leq \ldots \leq j_i \leq k} \right) \mu(p_{j_1} \cdots p_{j_i})\tau(p_{j_1} \cdots p_{j_i})$$
$$= \sum_{i=0}^{k} \binom{k}{i} (-1)^i 2^i = \sum_{i=0}^{k} \binom{k}{i} (-2)^i 1^{k-i} = (1-2)^k = (-1)^k.$$

ii. We easily compute that $2020 \equiv 4 \pmod 9$. Since $(4, 9) = 1$, Euler's theorem implies

$$4^{\phi(9)} = 4^6 \equiv 1 \pmod 9.$$

Using these facts, we compute

$$2020^{2021} \equiv 4^{2021} \equiv 4^{6\cdot 336+5} \equiv (4^6)^{336} \cdot 4^5 \equiv 4^5 \equiv 7 \pmod 9.$$ □

Question 3. Solve
$$4x^{19} + 10x^{13} + 7x^{10} + 3x^2 + 1 \equiv 0 \pmod{15}.$$

Answer. Set $f(x) = 4x^{19} + 10x^{13} + 7x^{10} + 3x^2 + 1$. We have that $15 = 3 \cdot 5$, so we split the original question to the system

$$\begin{cases} f(x) \equiv 0 \pmod 3, \\ f(x) \equiv 0 \pmod 5. \end{cases}$$

Since 3 is prime, Fermat's theorem yields $x^3 \equiv x \pmod 3$, for every $x \in \mathbb{Z}$. Thus, for every $x \in \mathbb{Z}$, we have that

$$\begin{aligned} f(x) &= 4x^{19} + 10x^{13} + 7x^{10} + 3x^2 + 1 \equiv x^{19} + x^{13} + x^{10} + 1 \\ &\equiv (x^3)^6 x + (x^3)^4 x + (x^3)^3 x + 1 \equiv x^7 + x^5 + x^4 + 1 \\ &\equiv (x^3)^2 x + x^3 x^2 + x^3 x + 1 \equiv x^3 + x^3 + x^2 + 1 \equiv x^2 + 2x + 1 \pmod 3. \end{aligned}$$

We easily verify (with tests) that the only solution of $x^2 + 2x + 1 \equiv 0 \pmod 3$ is $x \equiv 2 \pmod 3$.

We work similarly $\pmod 5$ and obtain:

$$\begin{aligned} f(x) &= 4x^{19} + 10x^{13} + 7x^{10} + 3x^2 + 1 \equiv 4x^{19} + 2x^{10} + 3x^2 + 1 \\ &\equiv 4(x^5)^3 x^4 + 2(x^5)^2 + 3x^2 + 1 \equiv 4x^7 + 2x^2 + 3x^2 + 1 \\ &\equiv 4x^5 x^2 + 1 \equiv 4x^3 + 1 \pmod 5. \end{aligned}$$

We easily verify (with tests) that the only solution of $4x^3 + 1 \equiv 0 \pmod 5$ is $x \equiv 1 \pmod 5$.

It follows that we have one solution $\pmod{15}$ of $f(x) \equiv 0 \pmod{15}$, which is the solution of the system

$$\begin{cases} x \equiv 2 \pmod 3, \\ x \equiv 1 \pmod 5. \end{cases}$$

The Chinese Remainder Theorem ensures the existence of a unique solution of the above $\pmod{15}$. Let x be that solution. We have that

$$x \equiv 2 \pmod 3 \Rightarrow x = 3\kappa + 2,$$

for some κ. Also

$$x \equiv 1 \pmod 5 \Rightarrow 3\kappa + 2 \equiv 1 \pmod 5 \Rightarrow \kappa \equiv 3 \pmod 5,$$

that is, $\kappa = 5\lambda + 3$. It follows that

$$x = 3(5\lambda + 3) + 2 = 15\lambda + 11 \Rightarrow x \equiv 11 \pmod{15}. \qquad \square$$

Question 4. Examine whether the equation

$$23x^2 - 17y^2 + 5z^2 = 0$$

has non-trivial integer solutions.

Answer. We first observe that the requirements to apply Legendre's theorem directly are met, since 23, 17 and 5 are distinct primes. It follows that the equation admits non-trivial solutions if and only if $23 \cdot 17$ is a quadratic residue $\pmod 5$, $-23 \cdot 5$ is a quadratic residue $\pmod{17}$ and $17 \cdot 5$ is a quadratic residue $\pmod{23}$.

Since 23, 17 and 5 are primes, the above is equivalent to

$$\left(\frac{23 \cdot 17}{5}\right) = \left(\frac{-23 \cdot 5}{17}\right) = \left(\frac{17 \cdot 5}{23}\right) = 1.$$

Using the known properties of the Legendre symbol, we easily verify that the above is true. $\square$