Fall 2021 – Math 328K – 55385

Homework 8 Solutions

Problem 1. What are the last four decimal digits of the number 11^{15999}?

Solution 1. Let $x = [11^{15999}]_{10000}$. We have

$$\phi(10000) = \phi(2^4)\phi(5^4) = (2^4 - 2^3)(5^4 - 5^3) = 4000,$$

so $x^{4000} = [1]$ for all $x \in (\mathbb{Z}/10000\mathbb{Z})^\times$. Now 11 and 10000 are coprime, so $[11] \in (\mathbb{Z}/10000\mathbb{Z})^\times$, and therefore

$$[11]x = [11]^{16000} = ([11]^{4000})^4 = [1]^4 = [1].$$

So $x = [11]^{-1}$. We could compute this with the extended Euclidean algorithm, but it's actually really easy to guess the Bezout coefficients in this case: $10000 - 909 \cdot 11 = 1$, so the Bezout coefficients of 10000 and 11 are 1 and -909. This means that

$$x = [11]^{-1} = [-909] = [9091],$$

so the last four digits of 11^{15999} are 9091.

Problem 2. Show the following facts about Euler's ϕ–function:

a) $\phi(n)$ is even for every $n \geq 3$,

b) $\phi(n^k) = n^{k-1}\phi(n)$ for all $n, k \in \mathbb{N}$,

c) $\phi(n) \geq \sqrt{n}$ for all $n \in \mathbb{N} \setminus \{2, 6\}$,

d) If $m \mid n$, then $\phi(m) \mid \phi(n)$.

Solution 2.

a) If $n = p^k$ is a prime power, then $\phi(p^k) = p^{k-1}(p-1)$. If p is odd, then $p - 1$ is even, and if $p = 2$ and $k \geq 2$, then p^{k-1} is even. So $\phi(p^k)$ is even unless $p^k = 2$. If $n \geq 3$ then the prime power decomposition of n always contains a prime power different from 2. Since ϕ is multiplicative, this is enough for $\phi(n)$ to be even.

b) We proved in class that $\phi(n)/n$ is the product $\prod_p(1 - p^{-1})$, where p goes through all prime divisors of n. But n^k has the same prime divisors as n, so $\phi(n^k)/n^k = \phi(n)/n$. Multiply by n^k to get the statement we want.

c) The function $f(x) = \frac{\sqrt{x}}{x-1}$ is decreasing if $x > 1$. Its values on the first few primes are $f(2) = \sqrt{2}$, $f(3) = \frac{\sqrt{3}}{2}$ and $f(5) = \frac{\sqrt{5}}{4}$. So $f(p) < 1$ for all primes $p \geq 3$ and $f(2)f(p) \leq f(2)f(5) = \frac{\sqrt{10}}{4} < 1$ for all primes $p \geq 5$.

Let n be a positive integer and $\mathcal{P}$ the set of its prime divisors. Then

$$\frac{\phi(n)}{n} = \prod_{p \in \mathcal{P}} \left(1 - \frac{1}{p}\right) = \prod_{p \in \mathcal{P}} \frac{1}{f(p)\sqrt{p}} = \frac{1}{\prod_{p \in \mathcal{P}} f(p)} \cdot \frac{1}{\sqrt{\prod_{p \in \mathcal{P}} p}} \geq \frac{1}{\prod_{p \in \mathcal{P}} f(p)} \cdot \frac{1}{\sqrt{n}}.$$

So if we can show that $\prod_{p \in \mathcal{P}} f(p) \leq 1$, then $\phi(n) \geq \sqrt{n}$ would follow. If $2 \notin \mathcal{P}$ then $f(p) < 1$ for all $p \in \mathcal{P}$, so $\prod_{p \in \mathcal{P}} f(p) \leq 1$. If $2 \in \mathcal{P}$ but $\mathcal{P}$ also contains a prime $q \geq 5$, then $\prod_{p \in \mathcal{P}} f(p) \leq f(2)f(q) < 1$.

The remaining cases are $\mathcal{P} = \{2\}$ and $\mathcal{P} = \{2, 3\}$. That is, $n = 2^i 3^j$ for integers $i \geq 1$ and $j \geq 0$. If $j = 0$ then $\phi(n) = 2^{i-1} = \frac{n}{2}$. If $j \geq 1$ then $\phi(n) = \phi(2^i)\phi(3^j) = 2^{i-1} \cdot 2 \cdot 3^{j-1} = \frac{n}{3}$.

If $n \geq 9$ then $\frac{n}{2} \geq \frac{n}{3} \geq \sqrt{n}$, so we are done, both in the case $j = 0$ and $j \geq 1$. The only remaining possibilities for n are $1, 2, 3, 4, 6, 8$. We directly compute

n	1	2	3	4	6	8
$\phi(n)^2$	1	1	4	4	4	16

So $\phi(n) \geq \sqrt{n}$ in all cases except $n = 2$ or $n = 6$.

d) First observe that, if p is a prime and $0 \leq j \leq i$, then $\phi(p^j) \mid \phi(p^i)$. If $j = 0$ this is trivially true, and otherwise $\phi(p^j) = p^{j-1}(p-1)$ is also a divisor of $\phi(p^i) = p^{i-1}(p-1)$.

Now write $n = p_1^{i_1} \cdots p_k^{i_k}$ for distinct primes $p_1, \ldots, p_k$ and $i_1, \ldots, i_k \geq 1$. If $m \mid n$, then $m = p_1^{j_1} \cdots p_k^{j_k}$ with $j_\ell \leq i_\ell$ for all ℓ. So $\phi(p_\ell^{j_\ell}) \mid \phi(p_\ell^{i_\ell})$ for all ℓ and therefore $\phi(m) \mid \phi(n)$.

Problem 3. Let $n = p_1 \cdots p_k$ be a product of distinct (odd) primes and let $x \in \mathbb{Z}/n\mathbb{Z}$. Show that

$$x^{\phi(n)+1} = x.$$

Solution 3. Let $y = x^{\phi(n)+1} - x$. We want to show that $y = [0]$. By the Chinese Remainder Theorem, it is enough to show that $y \bmod p_i = 0 \bmod p_i$ for all $i \in \{1, \ldots, k\}$. Since ϕ is multiplicative, we have $\phi(p_i) \mid \phi(n)$, say $\phi(n) = \phi(p_i)d_i$ for some (positive) integer d_i. So

$$y \bmod p_i = ((x \bmod p_i)^{\phi(p_i)})^{d_i}(x \bmod p_i) - (x \bmod p_i).$$

This is $[0]$ if $x \bmod p_i = [0]$, but also if $x \bmod p_i \neq [0]$ by Euler's Theorem.

Problem 4. Let $m \in \mathbb{N}$. The goal of this problem is to find all integers which are congruent modulo m to their own square. In other words, we want to find all solutions of the equation $x^2 - x = 0$ in $\mathbb{Z}/m\mathbb{Z}$.

a) Show that, if m is prime, then the only solutions are $[0]$ and $[1]$.

b) Show that, if m is a prime power, then the only solutions are still $[0]$ and $[1]$.

c) For general m, let $m = p_1^{i_1} \cdots p_k^{i_k}$ be the prime–power decomposition of m with $p_1 < \cdots < p_k$ prime and $i_1, \ldots, i_k \in \mathbb{N}$. Show there are 2^k different solutions of the equation $x^2 - x = 0$ in $\mathbb{Z}/m\mathbb{Z}$, and that these are given by

$$\sum_{j=1}^{k} \delta_j \left(\frac{m}{p_j^{i_j}} \right)^{p_j^{i_j} - p_j^{i_j - 1}} \mod m$$

for every tuple $(\delta_1, \ldots, \delta_k) \in \{0, 1\}^k$.

Hint: For the last part, use Euler's theorem and the Chinese remainder theorem.

Solution 4.

a) Clearly $[0]$ and $[1]$ are solutions of the equation $x^2 - x = 0$. Conversely, let $x = [a] \in \mathbb{Z}/m\mathbb{Z}$ with $x^2 - x = 0$. Then $m \mid a(a-1)$. Since m is prime, $m \mid a$ or $m \mid a - 1$. So $[a] = [0]$ or $[a] = [1]$.

b) Let $m = p^k$, p prime, $k \geq 2$. We can use Hensel's Lemma. The derivative of the polynomial $f(x) = x^2 - x$ is $f'(x) = 2x - 1$. So

$$\begin{aligned} f'(0) \bmod p &= -1 \bmod p \neq 0 \bmod p, \\ f'(1) \bmod p &= 1 \bmod p \neq 0 \bmod p. \end{aligned}$$

So by Hensel's Lemma both $[0]_p$ and $[1]_p$ have a unique lift to $\mathbb{Z}/p^2\mathbb{Z}$ which is a solution, these in turn have a unique lift to $\mathbb{Z}/p^3\mathbb{Z}$ etc. So there are exactly two solutions in $\mathbb{Z}/p^k\mathbb{Z}$, which we can directly verify to be $[0]$ and $[1]$.

c) By the Chinese Remainder Theorem there are 2^k solutions to the equation in $\mathbb{Z}/m\mathbb{Z}$, which we obtain as follows. If $[a_1]_{p_1^{i_1}}, \ldots, [a_k]_{p_k^{i_k}}$ are any solutions in $\mathbb{Z}/p_1^{i_1}\mathbb{Z}, \ldots, \mathbb{Z}/p_k^{i_k}\mathbb{Z}$, then

$$\sum_{j=1}^{k} a_j M_j y_j \mod m$$

is a solution in $\mathbb{Z}/m\mathbb{Z}$, where $M_j = m/p_j^{i_j}$ and y_j is any integer satisfying $[y_j]_{p_j^{i_j}} = [M_j]_{p_j^{i_j}}^{-1}$, and every solution is of this form. By Euler's Theorem we can choose $y_j = M_j^{\phi(p_j^{i_j})-1}$, since

$$[M_j^{\phi(p_j^{i_j})-1}]_{p_j^{i_j}} \cdot [M_j]_{p_j^{i_j}} = [M_j^{\phi(p_j^{i_j})}]_{p_j^{i_j}} = [1]_{p_j^{i_j}}.$$

So

$$\sum_{j=1}^{k} a_j M_j y_j \bmod m = \sum_{j=1}^{k} a_j M_j^{\phi(p_j^{i_j})} \bmod m = \sum_{j=1}^{k} a_j \left(\frac{m}{p_j^{i_j}}\right)^{p_j^{i_j} - p_j^{i_j - 1}} \bmod m.$$

By part b) we can choose each of the a_j to be in the set $\{0, 1\}$, and every such choice gives a different solution in $\mathbb{Z}/m\mathbb{Z}$.