Fall 2021 – Math 328K – 55385

Homework 6 Solutions

Problem 1. Using Fermat's little theorem, find the least positive residue of $2^{(10^6)}$ modulo 17.

Solution 1. By Fermat's little theorem, $x^{16} = [1]_{17}$ for all $x \in \mathbb{Z}/17\mathbb{Z} \setminus \{[0]_{17}\}$. Since $10^6 = 16 \cdot 62500$, we have

$$[2^{10^6}]_{17} = [2]_{17}^{10^6} = ([2]_{17}^{16})^{62500} = [1]_{17}^{62500} = [1]_{17},$$

so the least positive residue of 2^{10^6} modulo 17 is 1.

Problem 2. Show that, other than with ISBN-10, the check digit used for ISBN-13 does not protect against an arbitrary transposition of digits. Which transpositions can it detect?

Solution 2. Let $(x_1, \ldots, x_{13}) \in (\mathbb{Z}/10\mathbb{Z})^{13}$ be a valid ISBN-13 number. This means that

$$\sum_{k=1}^{13} a_k x_k = [0].$$

with $a_k = 2 + (-1)^k$. Let $(y_1, \ldots, y_{13}) \in (\mathbb{Z}/10\mathbb{Z})^{13}$ be the number obtained by applying one transposition to $(x_1, \ldots, x_{13})$, the one exchanging the i-th and j–th digits. So $y_i = x_j$, $y_j = x_i$ and $y_k = x_k$ for all $k \notin \{i, j\}$. Then

$$\sum_{k=1}^{13} a_k y_k = \sum_{k=1}^{13} (a_k y_k - a_k x_k) = a_i(y_i - x_i) + a_j(y_j - x_j) = (a_i - a_j)(y_i - x_i). \qquad (\star)$$

If i and j are both even or both odd, then $a_i = a_j$, so $(\star)$ evaluates to $[0]$. If i is even and j is odd, then $a_i - a_j = \pm 2$, so $(\star)$ evaluates to $[0]$ if and only if $x_i - y_i \in \{[0], [5]\}$.

So ISBN-13 detects a transposition of two digits if and only if they their indices have opposite parity and the values are different and their difference is not exactly 5.

Problem 3. Show that, if p is an odd prime, then

$$1^2 \cdot 3^2 \cdots (p-4)^2 \cdot (p-2)^2 \equiv (-1)^{(p+1)/2} \pmod p$$

Solution 3. Note that for every $[2i-1]_p = -[1-2i]_p = -[p-2i+1]_p = -[2(\frac{p+1}{2}-i)]_p$ for every $i \in \mathbb{Z}$. So

$$\begin{aligned}
\prod_{i=1}^{(p-1)/2} [2i-1]_p^2 &= (-1)^{(p-1)/2} \prod_{i=1}^{(p-1)/2} [2(\tfrac{p+1}{2}-i)]_p \prod_{i=1}^{(p-1)/2} [2i-1]_p \\
&= (-1)^{(p-1)/2} \prod_{i=1}^{(p-1)/2} [2i]_p \prod_{i=1}^{(p-1)/2} [2i-1]_p \\
&= (-1)^{(p-1)/2} \prod_{i=1}^{p-1} [i]_p
\end{aligned}$$

By Wilson's Theorem, $\prod_{i=1}^{p-1}[i]_p = [-1]_p$, so we get $\prod_{i=1}^{(p-1)/2}[2i-1]_p^2 = [(-1)^{(p+1)/2}]_p$.

Problem 4. You probably know that a positive integer is divisible by 3 or 9 if the sum of its digits is divisible by 3 or 9, respectively. The reason for this is that $10 \bmod 3 = 1 \bmod 3$ and $10 \bmod 9 = 1 \bmod 9$: suppose that the integer $x \in \mathbb{Z}_+$ has digits $x_0, x_1, \ldots, x_n$, ordered from the least significant to most significant, that is

$$x = \sum_{i=0}^{n} x_i \cdot 10^i.$$

Then

$$x \bmod 3 = \sum_{i=0}^{n} (x_i \bmod 3)(10 \bmod 3)^i = \sum_{i=0}^{n} (x_i \bmod 3)(1 \bmod 3)^i = \sum_{i=0}^{n} x_i \bmod 3.$$

So x is divisible by 3 if and only if $\sum_{i=0}^{n} x_i$ is.

a) Find a test like this for divisibility by 11 and divisibility by 101.

b) By the same method, try to find a test for divisibility by 5 and by 15.

c) This is an alternative way to construct a "general" divisibility test. Let $d \in \mathbb{Z}_+$ with $(d, 10) = 1$ and let $e \in \mathbb{Z}$ such that $[e]_d$ is an inverse of $[10]_d$. Show that $d \mid x$ if and only if $d \mid x'$, where
$$x' = \frac{x - x_0}{10} + e x_0.$$
Iterating this gives a sequence $x, x', x'', x''', \ldots$ whose terms are eventually small enough to check for divisibility directly.

Solution 4. For any positive integer $m \in \mathbb{Z}$ we have

$$x \bmod m = \sum_{i=0}^{n} (10 \bmod m)^i (x_i \bmod m),$$

so if $a_0, a_1, \dots \in \mathbb{Z}$ are integers with $[a_i]_m = [10]_m^i$, then x is divisible by m if and only if $\sum_{i=0}^{n} a_i x_i$ is divisible by m.

a) We have $[10]_{11}^i = [(-1)^i]_{11}$, so x is divisible by 11 if and only if $\sum_{i=0}^{n}(-1)^i x_i$ is divisible by 11. Similarly, $[10]_{101}^i$ gives the sequence

$$a_0, a_1, a_2, \dots = 1, 10, -1, -10, 1, 10, -1, -10, \dots$$

and x is divisible by 101 if and only if $\sum_{i=0}^{n} a_i x_i$ is divisible by 101. In words, this means we can split up the number in groups of two digits, starting with the least significant ones, and alternatingly add and subtract these two–digit numbers. The resulting number is divisible by 101 if and only if the original was.

Here is an example: 654783 is divisible by 101 since

$$65 - 47 + 83 = 101,$$

which is of course divisible by 101.

b) Since $[10]_5 = [0]_5$ we have $[10]_5^i = [0]_5$ for all $i \geq 1$, and $[10^0]_5 = [1]_5$. So x is divisible by 5 if and only if x_0 is divisible by 5.

The sequence $[10^i]_{15}$ for $i = 0, 1, 2, 3, \dots$ is $[1], [10], [10], [10], \dots$. So x is divisible by 15 if and only if

$$x_0 + 10 \sum_{i=1}^{n} x_i$$

is divisible by 15. For example, 972465 is divisible by 15:

$$9 + 7 + 2 + 4 + 6 = 28, \quad 28 \cdot 10 + 5 = 285,$$

so 972465 is divisible by 15 if and only if 285 is divisible by 15. Iterating this, 285 is divisible by 15 if and only if 105 is divisible by 15, if and only if 15 is divisible by 15. So $15 | 972465$.

c) With the setup from the question, observe that

$$[10]_d [x']_d = [x]_d - [x_0]_d + [10]_d [e]_d [x_0]_d = [x]_d.$$

Since $[10]_d$ is invertible, $[x']_d = [0]_d$ if and only if $[x]_d = [0]_d$, which is what we wanted to show.

If we wanted to see with this test whether 50933 is divisible by 31, we would first find $e \in \mathbb{Z}$ with $[e]_{31} = [10]_{31}^{-1}$, for example $e = -3$. Then

$$\begin{aligned} 31 \mid 50933 &\iff 31 \mid (5093 - 3 \cdot 3 = 5084) \\ &\iff 31 \mid (508 - 3 \cdot 4 = 496) \\ &\iff 31 \mid (49 - 3 \cdot 6 = 31) \end{aligned}$$

which is clearly true. Indeed, $50933 = 1643 \cdot 31$.

Problem 5. Let $m \in \mathbb{Z}_+$, $m > 2$, and let $(\mathbb{Z}/m\mathbb{Z})^\times = \{[a] \mid (a, m) = 1\}$ be the subset of all invertible elements in $\mathbb{Z}/m\mathbb{Z}$. Show that

$$\sum_{x \in (\mathbb{Z}/m\mathbb{Z})^\times} x = [0].$$

Solution 5. If x is invertible then $-x$ is also invertible (with inverse $-x^{-1}$). If $x \neq -x$ this pair of summands cancels, so it suffices to take the sum of all $x \in (\mathbb{Z}/m\mathbb{Z})^\times$ with $x = -x$, or equivalently $2x = [0]_m$.

The linear Diophantine equation $2x = [0]_m$ has a single solution $x = [0]_m$ if m is odd, and two solutions $x = [0]_m$ and $x = [m/2]_m$ if m is even.

Out of these $[0]_m$ is never invertible, and $[m/2]_m$ is invertible if and only if $(m/2, m) = 1$, which would only be the case if $m = 2$. But we explicitly excluded $m = 2$, so there are no invertible x with $2x = [0]_m$, hence the sum evaluates to $[0]$.