Homework 6

due Thursday, October 14, 14:00

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

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?

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

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

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.

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

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