

Homework 6

due Tuesday, October 15, 11:00

Problem 1.

- a) Show that $\overline{4}^n = \overline{3n+1}$ in \mathbb{Z}_9 for every $n \in \mathbb{N}$.
- b) More generally, show that

$$(a+1)^n \bmod a^2 = (an+1) \bmod a^2$$

for all $a, n \in \mathbb{N}$.

Problem 2. Let p be an odd prime and $a \in \mathbb{Z}_p$ with $a \neq \overline{0}$. A *square root* of a is a solution $x \in \mathbb{Z}_p$ of the equation $x^2 = a$.

- a) Show that every $a \in \mathbb{Z}_p \setminus \{\overline{0}\}$ has either none or exactly two square roots.
- b) Conclude that \mathbb{Z}_p has exactly two elements which are their own inverses.
- c) Find the square roots of all elements of \mathbb{Z}_7 , if they exist.
- d) Is the statement of a) still true if p is not prime?

Problem 3. 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 4. An electronics store wants to use standard UPC-A barcodes (which use the same check digits as ISBN-13) to label their products, but instead of using the registered article numbers they just decide to encode the price in cents directly in the barcode. To avoid confusion with real article numbers, they put the marker 0333 in front of it. For example, they sell a phone for \$379.00, which gets the code

0 333000 379006.

- a) Check that 6 is indeed the correct check digit, so this is a valid code.

b) Suppose we have sufficient criminal energy and a fineliner pen to manipulate the barcode. By the way barcodes work, adding lines allows us to do the following substitutions only¹:

$3 \mapsto 0$ $3 \mapsto 1$ $3 \mapsto 5$ $6 \mapsto 0$ $6 \mapsto 4$ $6 \mapsto 9$ $7 \mapsto 1$

$7 \mapsto 2$ $7 \mapsto 4$ $7 \mapsto 5$ $7 \mapsto 9$ $8 \mapsto 2$ $8 \mapsto 4$ $8 \mapsto 5$

Can we use these substitutions to manipulate the code to show a lower price, while still starting with 0333 and having a valid check digit? What is the lowest we can get?

¹actually these substitutions only work for the last 6 digits. See Wikipedia “Universal Product Code” or “International Article Number” if you’re interested in the details how barcodes work.