Math 300.2 Homework 4

Paul Hacking

October 9, 2017

Reading: Sundstrom, Sections 3.4, 3.5 and 4.1.

Justify your answers carefully.

(1) Suppose we are given an 8×8 chessboard and a collection of dominoes (2×1 tiles). Each domino can be used to cover two adjacent squares of the chessboard. Suppose we remove two opposite corner squares from the chessboard. Is it possible to cover the remaining squares using dominoes? (Either describe a tiling by dominoes or give a proof by contradiction that no tiling exists.)

[Hint: What colour are the squares we remove?]

(2) (a) Prove the following statement: For all integers a, the last digit of a^2 is either 0,1,4,5,6, or 9.

(b) We say an integer n is a *perfect square* if $n = m^2$ for some integer m. Is the integer 18446744073709551617 a perfect square?

[Hint: For a non-negative integer a, the last digit of a is equal to the remainder r when we divide a by 10, so $a \equiv r \bmod 10$. In class we showed that for all integers a, b, c, d and positive integers n, if $a \equiv b \bmod n$ and $c \equiv d \bmod n$ then $ac \equiv bd \bmod n$. As the special case $a = c$ and $b = d$ of this result, we deduce that for all integers a, b and positive integers n, if $a \equiv b \bmod n$ then $a^2 \equiv b^2 \bmod n$.]

(3) Prove the following statement: For all integers a, $a^2 \equiv 0, 1$ or $4 \bmod 8$.

(4) (a) Prove the following statement: For all integers a, if $3 \mid a^2$ then $3 \mid a$.

(b) Using part (a) or otherwise, prove that $\sqrt{3}$ is irrational.

[Hint: (a) Prove the contrapositive using cases and congruence notation. (b) Adapt the proof that $\sqrt{2}$ is irrational given in class.]

(5) Find all solutions of the following congruences.

(a) $x^3 + 1 \equiv 0 \bmod 3$.

(b) $x^2 + x + 3 \equiv 0 \bmod 5$.

(6) Prove that the equation

$$x^2 - 5y^3 = 23$$

has no integer solutions.

[Hint: Give a proof by contradiction and use congruence modulo n for a suitable positive integer n.]

(7) Recall that for all $a, b, c, d \in \mathbb{Z}$ and $n \in \mathbb{N}$, if $a \equiv b \bmod n$ and $c \equiv d \bmod n$ then $ac \equiv bd \bmod n$. Using this fact repeatedly, we deduce the following statement:

For all $a, b \in \mathbb{Z}$ and $m, n \in \mathbb{N}$, if $a \equiv b \bmod n$ then $a^m \equiv b^m \bmod n$.

(Later we will give a more careful explanation of this using mathematical induction.)

Using the above statement, compute (i) the remainder when 2018^{2018} is divided by 2017 and (ii) the remainder when 2017^{2017} is divided by 2018.

(8) Let n be a positive integer.

(a) Prove the following statement: For all integers x,

$$(n - x)^2 \equiv x^2 \bmod n.$$

(b) We say an integer r is a *quadratic residue* modulo n if $0 \leqslant r < n$ and there exists an integer x such that $x^2 \equiv r \bmod n$. Using part (a) or otherwise, show that the number of quadratic residues modulo n is at most $(n + 1)/2$ if n is odd and at most $n/2 + 1$ if n is even.

(c) Give a proof or a counterexample for the following statement: For every positive integer n, the number of quadratic residues modulo n is equal to $(n+1)/2$ if n is odd and is equal to $n/2+1$ if n is even.