PROBLEM SET 2

18.781 SPRING 2023

Due Monday, February 27. You may consult books, papers, and websites as long as you cite them and write up your solutions in your own words. Do not request answers on forums online. To get full points on a proof-based problem, *please write in complete sentences.*

Book. (Stillwell, *Elements of Number Theory*)

(1) 2.3.1–2.3.2
(2) 2.4.1 ("infinite descent" means your proof should invoke well-ordering)
(3) 2.5.1–2.5.2
(4) 2.5.4–2.5.5
(5) 2.6.2–2.6.4
(6) 3.2.1
(7) 3.2.2–3.2.3
(8) 3.3.1–3.3.4 (here, $a \not\equiv 0 \pmod{p}$)
(9) 3.4.1–3.4.2
(10) 3.4.3–3.4.4
(11) 3.4.5

Non-Book. Problems 1 and 4 require the *prime divisor property* on Stillwell page 29. *(2/26: Typo fixed)*

Problem 1. Use the well-ordering principle and the prime divisor property to prove that $x_1^2 = 2x_2^2$ has no solutions $x_1, x_2 \in \mathbf{N}$.

Problem 2. Use congruence arithmetic to prove that, for any $r \in \mathbf{Z}$, the numbers $(20 + r)^2$ and $(30 - r)^2$ have the same last two digits in base ten.

Problem 3. Prove the following rule for testing divisibility-by-7:

> Let $n = 10q + r$, where $q, r \in \mathbf{N}_0$ and $r < 10$. Then 7 divides n if and only if 7 divides $q + 5r$.

(*Hint:* Rescale one of the expressions.) This rule made the news a few years ago, when it was rediscovered by a young boy living in the UK.

Problem 4. Let $p > 2$ be prime.

(1) Use the prime divisor property to prove that the only solutions to the congruence $x^2 \equiv a^2 \pmod{p}$ are $x \equiv \pm a \pmod{p}$.
(2) Use (1) to prove that exactly half of the nonzero residues modulo p take the form $a^2 \pmod{p}$ for some $a \in \mathbf{Z}$.
(3) Use (2) to prove that if $x^2 \equiv A \pmod{p}$ and $x^2 \equiv B \pmod{p}$ have no solutions for x, then $x^2 = AB \pmod{p}$ must have a solution. (*Hint:* Look at Stillwell exercise 3.3.3 for inspiration.)