Midterm #1: practice

MATH 311 — Intro to Number Theory
Midterm: Thursday, Oct 4

Please print your name:

Problem 1. Find $d = \gcd(119, 272)$. Using the Euclidean algorithm, find integers x, y such that $119x + 272y = d$.

(Use Homework Problems 1.1, 1.2, 1.3 to generate more practice problems of this kind.)

Problem 2.

(a) For which values of k has the diophantine equation $123x + 360y = k$ at least one integer solution?

(b) Determine all solutions of $123x + 360y = 99$ with x and y positive integers.

(Use Homework Problems 1.7, 1.8 to generate more practice problems of this kind.)

Problem 3.

(a) Using binary exponentiation, compute $31^{41} \pmod{23}$.

(b) Without computations, determine $31^{41} \pmod{41}$.

(c) Is $314^{159} + 265^{358} + 10$ divisible by 19?

(Use Homework Problems 3.3, 3.4 to generate more practice problems of this kind.)

Problem 4.

(a) Find the modular inverse of 17 modulo 23.

(b) Solve $15x \equiv 7 \pmod{31}$.

(c) List all invertible residues modulo 10.

(d) How many solutions does $16x \equiv 1 \pmod{70}$ have modulo 70? Find all solutions.

(e) How many solutions does $16x \equiv 4 \pmod{70}$ have modulo 70? Find all solutions.

(Use Homework Problems 2.6, 2.7, 2.8, 2.9 to generate more practice problems of this kind.)

Problem 5. Solve the following system of congruences:

$$\begin{aligned} 3x + 5y &\equiv 6 \pmod{25} \\ 2x + 7y &\equiv 2 \pmod{25} \end{aligned}$$

(Use Homework Problems 2.10, 2.11 to generate more practice problems of this kind.)

Problem 6. Spell out a precise version of the following famous results:

(a) Bézout's identity

(b) Fermat's little theorem

Armin Straub
straub@southalabama.edu

Problem 7.

(a) Let a, n be positive integers. Show that a has a modular inverse modulo n if and only if $\gcd(a, n) = 1$.

(b) Let p be a prime, and a an integer such that $p \nmid a$. Show that the modular inverse a^{-1} exists, and that

$$a^{-1} \equiv a^{p-2} \pmod{p}.$$

(c) Compute $17^{-1} \pmod{101}$ in two different ways:

- Using Bézout's identity.
- Using the previous part of this problem and binary exponentiation.

Problem 8.

(a) Determine $\operatorname{lcm}(81, 135)$.

(Use Homework Problem 1.6 to generate more practice problems of this kind.)

(b) The residues $-2, -9, 6, 17, -10$ do not form a complete set of residues modulo 6. Which residue is missing?

(Use Homework Problem 2.5 to generate more practice problems of this kind.)

(c) Express 3141 in base 6.

(Use Homework Problems 3.1, 3.2 to generate more practice problems of this kind.)

(d) Determine, without the help of a calculator, the remainder of 112358132134 modulo 9.

(Use Homework Problem 2.6 to generate more practice problems of this kind.)

(e) What is the remainder of 62831853 modulo 11?

(Use Homework Problem 2.7 to generate more practice problems of this kind.)

Problem 9. We call (a, b, c) a prime triple if a, b, c are all primes.

(a) List the first few prime triples of the form $(p, p+2, p+6)$.
(It is believed, but nobody can show, that there are infinitely many such triples.)

(b) Show that there is only a single prime triple of the form $(p, p+2, p+4)$.

(c) Show that there are no prime triples of the form $(p, p+2, p+5)$.

Armin Straub
straub@southalabama.edu