Midterm #2: practice

MATH 311 — Intro to Number Theory
midterm: Thursday, Oct 20

Please print your name:

Calculators will not be permitted on the exam. The numbers on the exam will be suitable for calculating by hand.

Problem 1.

(a) Express 3141 in base 6.

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

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

(d) Is $0, 1, 2, 4, 8, \ldots, 2^{11}$ a complete set of residues modulo 13?

(e) Is 2 a primitive root modulo 11? What about 3?

Do you see a way to determine all primitive roots modulo 11 without much further computation?

Problem 2.

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

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

(c) Show that $314^{159} + 265^{358} + 10$ is divisible by 19.

Problem 3.

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

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

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

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

Problem 4. Solve the following system of congruences:

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

Problem 5.

(a) Solve $x \equiv 1 \pmod{3}$, $x \equiv 2 \pmod{4}$, $x \equiv 3 \pmod{5}$, $x \equiv 4 \pmod{11}$.

(b) Solve $x \equiv 1 \pmod{3}$, $x \equiv 2 \pmod{4}$, $2x \equiv 3 \pmod{5}$, $3x \equiv 4 \pmod{11}$.

(c) Find the smallest integer $a > 2$ such that $2|a$, $3|(a+1)$, $4|(a+2)$ and $5|(a+3)$.

— There is two more problems on the second page... —

Armin Straub
straub@southalabama.edu

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

(a) Bézout's identity

(b) Fermat's little theorem

(c) Chinese remainder theorem

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 the modular inverse of 17 modulo 101 in two different ways:

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

— It is also a very good idea to review the problems from Homework 4. —

Armin Straub
straub@southalabama.edu