Midterm #2

MATH 311 — Intro to Number Theory
Thursday, Oct 20

Please print your name:

No notes or tools of any kind are permitted. There are 25 points in total. You need to show work to receive full credit.

Good luck!

Problem 1. (warmup, 4 points)

(a) The remainder of 10202017 modulo 11 is $\boxed{}$.

(b) Complete the following to a complete set of residues modulo 7: $\boxed{-4, -2, -1, 2, 4, 8, }$

(c) The number 51 in base 7 is $\boxed{}$.

(d) List all primitive roots modulo 5: $\boxed{}$

Solution.

(a) $10202017 \equiv 7 - 1 + 0 - 2 + 0 - 2 + 0 - 1 = 1 \pmod{11}$. Hence, the remainder of 10202017 modulo 11 is 1.

(b) $-4, -2, -1, 2, 4, 8, 0$ (a number congruent to 0 modulo 7 was missing)

(c) $51 = 7^2 + 2 = (102)_7$

(d) $2^0 = 1, 2^1 = 2, 2^2 = 4, 2^3 \equiv 3$, so 2 is a primitive root.

$3^0 = 1, 3^1 = 3, 3^2 = 4, 3^3 \equiv 2$, so 3 is a primitive root.

$4^0 = 1, 4^1 = 4, 4^2 = 1$, so 4 is not a primitive root.

Hence, primitive roots modulo 5 are $2, 3$. □

Problem 2. (warmup, 2 points) Carefully state Fermat's little theorem.

Solution. Let p be a prime, and suppose that $p \nmid a$. Then

$$a^{p-1} \equiv 1 \pmod{p}.$$ □

Problem 3. (3 points) Determine whether $31^{41} + 59^{26} + 53^5$ is divisible by 5. Carefully show your steps!

Solution. $31^{41} + 59^{26} + 53^5 \equiv 1^{41} + (-1)^{26} + 3^5 \equiv 1 + 1 + 3 \equiv 0 \pmod{5}$. Hence, $31^{41} + 59^{26} + 53^5$ is divisible by 5. Note that $3^5 \equiv 3 \pmod{5}$ by Fermat's little theorem. □

Armin Straub
straub@southalabama.edu

Problem 4. (3+1 points)

(a) Find the modular inverse of 10 modulo 43.

(b) Solve $10x \equiv 4 \pmod{43}$.

Solution.

(a) We use the extended euclidean algorithm:

$\underbrace{\gcd(10,43)}_{43=4\cdot 10+3} = \underbrace{\gcd(3,10)}_{10=3\cdot 3+1} = \gcd(1,3) = 1$, and Bézout's identity takes the form $1 = 10 - 3\cdot \underbrace{3}_{3=43-4\cdot 10} = 13\cdot 10 - 3\cdot 43$.

Hence, $13\cdot 10 \equiv 1 \pmod{43}$. In other words, $10^{-1} \equiv 13 \pmod{43}$.

(b) $10x \equiv 4 \pmod{43}$ has the unique solution $x \equiv 10^{-1}\cdot 4 \equiv 13\cdot 4 \equiv 9 \pmod{43}$. □

Problem 5. (4 points) Solve the following system of congruences:

$$\begin{aligned} 3x - y &\equiv 1 \pmod{15} \\ x + 2y &\equiv 4 \pmod{15} \end{aligned}$$

Solution. By any method we like, we find that the two equations $3x - y = 1$, $x + 2y = 4$ are solved by $x = \frac{6}{7}$, $y = \frac{11}{7}$

[For instance, $\begin{bmatrix} x \\ y \end{bmatrix} = \begin{bmatrix} 3 & -1 \\ 1 & 2 \end{bmatrix}^{-1} \begin{bmatrix} 1 \\ 4 \end{bmatrix} = \frac{1}{7}\begin{bmatrix} 2 & 1 \\ -1 & 3 \end{bmatrix}\begin{bmatrix} 1 \\ 4 \end{bmatrix} = \frac{1}{7}\begin{bmatrix} 6 \\ 11 \end{bmatrix}$.]

We note that $7^{-1} \equiv -2 \pmod{15}$.

Hence, our two congruences are solved by $\begin{bmatrix} x \\ y \end{bmatrix} \equiv \begin{bmatrix} 7^{-1}\cdot 6 \\ 7^{-1}\cdot 11 \end{bmatrix} \equiv \begin{bmatrix} -12 \\ -22 \end{bmatrix} \equiv \begin{bmatrix} 3 \\ 8 \end{bmatrix} \pmod{15}$. □

Armin Straub
straub@southalabama.edu

Problem 6. (3 points) Using binary exponentiation, compute $6^{13} \pmod{17}$. Carefully show all steps!

Solution. $6^2 \equiv 2 \pmod{17}$, $6^4 \equiv 2^2 = 4 \pmod{17}$, $6^8 \equiv 4^2 \equiv -1 \pmod{17}$

Hence, $6^{13} = 6^8 \cdot 6^4 \cdot 6 \equiv -1 \cdot 4 \cdot 6 \equiv 10 \pmod{17}$. □

Problem 7. (4+1 points)

(a) Find the smallest positive integer x simultaneously solving the three congruences
$$\begin{aligned} x &\equiv 1 \pmod{3}, \\ x &\equiv 4 \pmod{7}, \\ x &\equiv 1 \pmod{10}. \end{aligned}$$

(b) The next largest solution x to the above congruences is $\boxed{}$.

Solution. We break the problem into three pieces:

- $x \equiv 1 \pmod{3}$, $x \equiv 0 \pmod{7}$, $x \equiv 0 \pmod{10}$.

  Since x has to be of the form $x = 70z$, we solve $70z \equiv 1 \pmod{3}$ and find $z = 1$. Hence, $x = 70$ does the trick.

- $x \equiv 0 \pmod{3}$, $x \equiv 1 \pmod{7}$, $x \equiv 0 \pmod{10}$.

  Since x has to be of the form $x = 30z$, we solve $30z \equiv 1 \pmod{7}$ and find $z = 4$. Hence, $x = 120$ does the trick.

- $x \equiv 0 \pmod{3}$, $x \equiv 0 \pmod{7}$, $x \equiv 1 \pmod{10}$.

  Since x has to be of the form $x = 21z$, we solve $21z \equiv 1 \pmod{10}$ and find $z = 1$. Hence, $x = 21$ does the trick.

(a) Combining these three, $x \equiv 1 \pmod{3}$, $x \equiv 4 \pmod{7}$, $x \equiv 1 \pmod{10}$ is solved by $x = 70 + 4 \cdot 120 + 21 = 571$.

The solution is unique modulo $3 \cdot 7 \cdot 10 = 210$, and $571 \equiv 151 \pmod{210}$. Hence, $x = 151$ is the smallest positive integer simultaneously solving the three congruences.

(b) $151 + 210 = 361$ is the next largest solution.

□

(extra scratch paper)