Midterm #1

MATH 311 — Intro to Number Theory
Thursday, Oct 4

Please print your name:

No notes or tools of any kind are permitted. There are 28 points in total. You need to show work to receive full credit.

Good luck!

Problem 1. (4+2+2 points)

(a) Let $d = \gcd(17, 23)$. Using the Euclidean algorithm, find integers x, y such that $17x + 23y = d$.

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

(c) Solve $17x \equiv 10 \pmod{23}$.

Solution.

(a) We apply the extended Euclidean algorithm:

$$\begin{array}{lll} \gcd(17,23) & \boxed{23} = 1 \cdot \boxed{17} + 6 & \text{or: } \boxed{A} \quad 6 = 1 \cdot \boxed{23} - 1 \cdot \boxed{17} \\ = \gcd(6,17) & \boxed{17} = 3 \cdot \boxed{6} - 1 & \boxed{B} \quad 1 = -1 \cdot \boxed{17} + 3 \cdot \boxed{6} \\ = 1 & & \end{array}$$

Backtracking through this, we find that Bézout's identity takes the form

$$1 \underset{\boxed{B}}{=} -1 \cdot \boxed{17} + 3 \cdot \boxed{6} \underset{\boxed{A}}{=} 3 \cdot \boxed{23} - 4 \cdot \boxed{17}$$

In summary, we have $1 = -4 \cdot 17 + 3 \cdot 23$ (that is, $d = 1$, $x = -4$, $y = 3$).

(b) From the previous part, $17^{-1} \equiv -4 \pmod{23}$.

(c) $17x \equiv 10 \pmod{23}$ has the unique solution $x \equiv 17^{-1} \cdot 10 \equiv -4 \cdot 10 = -40 \equiv 6 \pmod{23}$. □

Armin Straub
straub@southalabama.edu

Problem 2. (9 points)

(a) The remainder of 124816 modulo 11 is $\boxed{}$.

(b) $5^{-1} \pmod 7$ is $\boxed{}$.

(c) Complete the following to a complete set of residues modulo 6: $\boxed{3, -1, 6, 8, 4, }$

(d) The number 55 in base 5 is $\boxed{}$.

(e) List all invertible residues modulo 12: $\boxed{}$

(f) The residue x is invertible modulo n if and only if $\boxed{}$.

(g) For which values of k has the diophantine equation $21x + 6y = k$ at least one integer solution?

$\boxed{}$

(h) How many solutions does $3x \equiv 2 \pmod{50}$ have modulo 50? $\boxed{}$

How many solutions does $5x \equiv 2 \pmod{50}$ have modulo 50? $\boxed{}$

How many solutions does $5x \equiv 20 \pmod{50}$ have modulo 50? $\boxed{}$

Solution.

(a) $124816 \equiv 6 - 1 + 8 - 4 + 2 - 1 = 10 \pmod{11}$. Hence, the remainder of 124816 modulo 11 is 10.

(b) $5^{-1} \equiv 3 \pmod 7$

(c) Note that, modulo 6, $3, -1, 6, 8, 4 \equiv 3, 5, 0, 2, 4$. Hence, the missing residue is 1.

(d) $55 = 2 \cdot 5^2 + 5 = (210)_5$

(e) $1, 5, 7, 11$

(f) The residue x is invertible modulo n if and only if $\gcd(x, n) = 1$.

(g) The diophantine equation $21x + 6y = k$ has a solution if and only if k is a multiple of $\gcd(21, 6) = 3$.

(h) $1, 0, 5$ □

Problem 3. (2 points) Carefully state Fermat's little theorem.

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

$$a^{p-1} \equiv 1 \pmod p.$$ □

Armin Straub
straub@southalabama.edu

Problem 4. (5 points) Determine $40^{1612} \pmod{17}$. Carefully show all steps!

Solution. First, we simplify base and exponent $40^{1612} \equiv 6^{1612} \equiv 6^{12} \pmod{17}$. For the second congruence, we used Fermat's little theorem and $1612 \equiv 12 \pmod{16}$.

We now use binary exponentiation: $6^2 \equiv 2 \pmod{17}$, $6^4 \equiv 2^2 = 4 \pmod{17}$, $6^8 \equiv 4^2 \equiv -1 \pmod{17}$

It follows that $6^{12} = 6^8 \cdot 6^4 \equiv -1 \cdot 4 \equiv -4 \pmod{17}$.

In conclusion, $40^{1612} \equiv -4 \pmod{17}$. □

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

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

Solution. By any method we like, we find that the two equations $2x + y = 3$, $x - 3y = 1$ are solved by $x = \frac{10}{7}$, $y = \frac{1}{7}$

[For instance, $\begin{bmatrix} x \\ y \end{bmatrix} = \begin{bmatrix} 2 & 1 \\ 1 & -3 \end{bmatrix}^{-1} \begin{bmatrix} 3 \\ 1 \end{bmatrix} = \frac{1}{-7} \begin{bmatrix} -3 & -1 \\ -1 & 2 \end{bmatrix} \begin{bmatrix} 3 \\ 1 \end{bmatrix} = \frac{1}{7} \begin{bmatrix} 10 \\ 1 \end{bmatrix}$.]

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

Hence, our two congruences are solved by $\begin{bmatrix} x \\ y \end{bmatrix} \equiv \begin{bmatrix} 7^{-1} \cdot 10 \\ 7^{-1} \cdot 1 \end{bmatrix} \equiv \begin{bmatrix} -20 \\ -2 \end{bmatrix} \equiv \begin{bmatrix} -5 \\ -2 \end{bmatrix} \pmod{15}$. □

Armin Straub
straub@southalabama.edu

(extra scratch paper)