Midterm #1

MATH 311 — Intro to Number Theory
Thursday, Oct 3

Please print your name:

No notes or tools of any kind are permitted. There are 33 points in total. You need to show work to receive full credit.

Good luck!

Problem 1. (4+2+2 points)

(a) Let $d = \gcd(16, 23)$. Using the Euclidean algorithm, find integers x, y such that $16x + 23y = d$.

(b) Find the modular inverse of 16 modulo 23.

(c) Solve $16x \equiv 3 \pmod{23}$.

Solution.

(a) We apply the extended Euclidean algorithm:

$$\begin{array}{ll} \gcd(16,23) & \boxed{23} = 1 \cdot \boxed{16} + 7 \\ = \gcd(7,16) & \boxed{16} = 2 \cdot \boxed{7} + 2 \\ = \gcd(2,7) & \boxed{7} = 3 \cdot \boxed{2} + 1 \\ = 1 & \end{array}$$

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

$$\begin{aligned} 1 &= \boxed{7} - 3 \cdot \boxed{2} = \boxed{7} - 3 \cdot \left(\boxed{16} - 2 \cdot \boxed{7}\right) = 7 \cdot \boxed{7} - 3 \cdot \boxed{16} \\ &= 7 \cdot \left(\boxed{23} - \boxed{16}\right) - 3 \cdot \boxed{16} = 7 \cdot \boxed{23} - 10 \cdot \boxed{16} \end{aligned}$$

In summary, we have $1 = -10 \cdot 16 + 7 \cdot 23$ (that is, $d = 1$, $x = -10$, $y = 7$).

(b) From the previous part, $16^{-1} \equiv -10 \pmod{23}$.

(c) $16x \equiv 3 \pmod{23}$ has the unique solution $x \equiv 16^{-1} \cdot 3 \equiv -10 \cdot 3 \equiv -7 \pmod{23}$. □

Armin Straub
straub@southalabama.edu

Problem 2. (10 points)

(a) The remainder of 314159 modulo 11 is $\square$.

(b) $2^{-1} \pmod{19}$ is $\square$.

(c) Complete the following to a complete set of residues modulo 5: $11, -10, 9, 2, \square$

(d) The number 26 in base 2 is $\square$.

(e) The number 26 in base 3 is $\square$.

(f) List all invertible residues modulo 12: $\square$

(g) The residue x is invertible modulo n if and only if $\square$.

(h) For which values of k has the diophantine equation $15x + 9y = k$ at least one integer solution?

$\square$

(i) How many solutions does $7x \equiv 12 \pmod{60}$ have modulo 60? $\square$

How many solutions does $6x \equiv 12 \pmod{60}$ have modulo 60? $\square$

How many solutions does $6x \equiv 2 \pmod{60}$ have modulo 60? $\square$

(j) Up to x, there are roughly $\square$ many primes.

Solution.

(a) $314159 \equiv 9 - 5 + 1 - 4 + 1 - 3 = -1 \equiv 10 \pmod{11}$. Hence, the remainder of 314159 modulo 11 is 10.

(b) $2^{-1} \equiv 10 \pmod{19}$

(c) Note that, modulo 5, $11, -10, 9, 2 \equiv 1, 0, 4, 2$. Hence, the missing residue is 3.

(d) $26 = (11010)_2$

(e) $26 = (222)_3$

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

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

(h) The diophantine equation $15x + 9y = k$ has a solution if and only if k is a multiple of $\gcd(15, 9) = 3$.

(i) $1, 6, 0$

(j) Up to x, there are roughly $x/\ln(x)$ many primes. □

Armin Straub
straub@southalabama.edu

Problem 3. (5 points) Determine $25^{3630} \pmod{19}$. Carefully show all steps!

Solution. First, we simplify base and exponent $25^{3630} \equiv 6^{3630} \equiv 6^{12} \pmod{19}$. For the second congruence, we used Fermat's little theorem and $3630 \equiv 30 \equiv 12 \pmod{18}$.

We now use binary exponentiation: $6^2 \equiv -2 \pmod{19}$, $6^4 \equiv (-2)^2 = 4 \pmod{19}$, $6^8 \equiv 4^2 \equiv -3 \pmod{19}$

It follows that $6^{12} = 6^8 \cdot 6^4 \equiv -3 \cdot 4 \equiv 7 \pmod{19}$.

In conclusion, $25^{3630} \equiv 7 \pmod{19}$. □

Problem 4. (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 $\begin{bmatrix} x \\ y \end{bmatrix} \equiv \begin{bmatrix} 7^{-1} \cdot 10 \\ 7^{-1} \cdot 1 \end{bmatrix} \equiv \begin{bmatrix} -20 \\ -2 \end{bmatrix} \equiv \begin{bmatrix} -5 \\ -2 \end{bmatrix} \pmod{15}$. □

Problem 5. (6 points) Using the Chinese remainder theorem, determine all solutions to $x^2 \equiv 1 \pmod{55}$.

Solution. By the CRT:

$$\begin{aligned} & x^2 \equiv 1 \pmod{55} \\ \iff\ & x^2 \equiv 1 \pmod{5} \text{ and } x^2 \equiv 1 \pmod{11} \\ \iff\ & x \equiv \pm 1 \pmod{5} \text{ and } x \equiv \pm 1 \pmod{11} \end{aligned}$$

Hence, there are four solutions $\pm 1, \pm a$ modulo 55. To find one of the nontrivial ones, we solve the congruences $x \equiv 1 \pmod{5}$, $x \equiv -1 \pmod{11}$:

$$x \equiv 1 \cdot 11 \cdot \underbrace{11^{-1}_{\bmod 5}}_{1} - 1 \cdot 5 \cdot \underbrace{5^{-1}_{\bmod 11}}_{-2} \equiv 11 + 10 = 21 \pmod{55}$$

Hence, we conclude that $x^2 \equiv 1 \pmod{55}$ has the four solutions $\pm 1, \pm 21 \pmod{55}$. □

Armin Straub
straub@southalabama.edu

(extra scratch paper)