# Midterm #1: practice

**MATH 311 — Intro to Number Theory**
**Midterm: Thursday, Oct 3**

***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 1.3, 1.4, 1.5 to generate more practice problems of this kind.)

**Solution.** We use the extended Euclidean algorithm:

$$\begin{aligned} & \gcd(119, 272) && \boxed{272} &&= 2 \cdot \boxed{119} + 34 \\ = \ & \gcd(34, 119) && \boxed{119} &&= 3 \cdot \boxed{34} + 17 \\ = \ & \gcd(17, 34) = 17 \end{aligned}$$

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

$$17 = \boxed{119} - 3 \cdot \boxed{34} = \boxed{119} - 3 \cdot \big(\boxed{272} - 2\boxed{119}\big) = 7 \cdot \boxed{119} - 3 \cdot \boxed{272}.$$

So, here, $d = 17$ as well as $x = 7$ and $y = -3$.

**Note.** Other values also work for $x$ and $y$. In fact, we know that the general solution is $\begin{bmatrix} x \\ y \end{bmatrix} = \begin{bmatrix} 7 \\ -3 \end{bmatrix} + \begin{bmatrix} 272/17 \\ -119/17 \end{bmatrix} t$. □

**Problem 2.**

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

(b) Determine the general solution to the diophantine equation $123x + 360y = 99$.

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

(Use Homework Problems 2.1, 2.2, 2.3 to generate more practice problems of this kind.)

**Solution.**

(a) We first compute $\gcd(123, 360)$ and find

$$\underbrace{\gcd(123, 360)}_{360 = 2 \cdot 123 + 114} = \underbrace{\gcd(114, 123)}_{123 = 1 \cdot 114 + 9} = \underbrace{\gcd(9, 114)}_{114 = 12 \cdot 9 + 6} = \underbrace{\gcd(6, 9)}_{9 = 1 \cdot 6 + 3} = \gcd(3, 6) = 3.$$

We therefore see that the diophantine equation $123x + 360y = k$ has at least one integer solution if and only if $k$ is a multiple of 3.

(b) Since $3 | 99$, the diophantine equation $123x + 360y = 99$ has solutions. We first divide out the common factor of 3 to get the simplified equation $41x + 120y = 33$.

(c) We already know that $\gcd(41, 120) = 1$. To find integers $x, y$ such that $41x + 120y = 1$, we use the extended Euclidean algorithm:

$$\begin{aligned} & \gcd(41, 120) && \boxed{120} &&= 3 \cdot \boxed{41} - 3 \\ = \ & \gcd(3, 41) && \boxed{41} &&= 14 \cdot \boxed{3} - 1 \\ = \ & 1 \end{aligned}$$

Armin Straub
straub@southalabama.edu

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

$$1 = -\boxed{41} + 14 \cdot \boxed{3} = -\boxed{41} + 14 \cdot \big(3 \cdot \boxed{41} - \boxed{120}\big) = 41 \cdot \boxed{41} - 14 \cdot \boxed{120}.$$

Hence, $41x + 120y = 1$ has the particular solution $\left[\begin{smallmatrix} x \\ y \end{smallmatrix}\right] = \left[\begin{smallmatrix} 41 \\ -14 \end{smallmatrix}\right]$.

Consequently, $41x + 120y = 33$ has the general solution $\left[\begin{smallmatrix} x \\ y \end{smallmatrix}\right] = 33\left[\begin{smallmatrix} 41 \\ -14 \end{smallmatrix}\right] + \left[\begin{smallmatrix} 120 \\ -41 \end{smallmatrix}\right]t$ with $t \in \mathbb{Z}$.

(d) From the previous part, we know that the general solution is $\left[\begin{smallmatrix} x \\ y \end{smallmatrix}\right] = 33\left[\begin{smallmatrix} 41 \\ -14 \end{smallmatrix}\right] + \left[\begin{smallmatrix} 120 \\ -41 \end{smallmatrix}\right]t$.

However, we are only interested in solutions with $x > 0$ and $y > 0$. $x > 0$ means $t > -\frac{33 \cdot 41}{120} = -12 + \frac{29}{40}$ (that is, $t \in \{-11, -10, -9, ...\}$), while $y > 0$ means $t < -\frac{33 \cdot 14}{41} = -12 + \frac{30}{41}$ (that is, $t \in \{-12, -13, -14, ...\}$). These conditions contradict each other, which means that there are no solutions with both $x$ and $y$ positive integers. □

**Problem 3.**

(a) Determine $31^{4441} \pmod{23}$, carefully showing all steps.

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

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

**Solution.**

(a) First, we simplify base and exponent $31^{4441} \equiv 8^{4441} = 8^{19} \pmod{23}$. For the second congruence, we used Fermat's little theorem and $4441 \equiv 41 \equiv 19 \pmod{22}$.

We now use binary exponentiation: $8^2 = 64 \equiv -5 \pmod{23}$, $8^4 \equiv (-5)^2 \equiv 2$, $8^8 \equiv 2^2 = 4$, $8^{16} \equiv 4^2 = 16$.

Hence, $31^{4441} \equiv 8^{19} = 8^{16} \cdot 8^2 \cdot 8^1 \equiv 16 \cdot \underbrace{(-5) \cdot 8}_{\equiv 6} \equiv 4 \pmod{23}$.

(b) $314^{159} + 265^{358} + 10 \equiv 10^{159} + (-1)^{358} + 10 \equiv 10^{159} + 11 \pmod{19}$

On the other hand, by Fermat's little theorem $10^{159} \equiv 10^{15} \pmod{19}$ because $159 \equiv 15 \pmod{18}$.

We now use binary exponentiation: $10^2 = 100 \equiv 5 \pmod{19}$, $10^4 \equiv 5^2 \equiv 6 \pmod{19}$, $10^8 \equiv 6^2 \equiv -2 \pmod{19}$.

Hence, $10^{15} = 10^8 \cdot 10^4 \cdot 10^2 \cdot 10^1 \equiv \underbrace{(-2) \cdot 6}_{\equiv 7} \cdot \underbrace{5 \cdot 10}_{\equiv -7} \equiv -49 \equiv 8 \pmod{19}$.

Combined, we find that $314^{159} + 265^{358} + 10 \equiv 10^{15} + 11 \equiv 8 + 11 \equiv 0 \pmod{19}$.

Consequently, $314^{159} + 265^{358} + 10$ is divisible by 19. □

**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 2.8, 2.9, 2.10, 2.11, 2.12 to generate more practice problems of this kind.)

Armin Straub
straub@southalabama.edu

**Solution.**

(a) We use the extended Euclidean algorithm:

$$\begin{array}{rll} & \gcd(17,23) & \boxed{23} = 1\cdot\boxed{17}+6 \\ = & \gcd(6,17) & \boxed{17} = 3\cdot\boxed{6}-1 \\ = & 1 & \end{array}$$

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

$$1 = 3\cdot\boxed{6} - \boxed{17} = 3\cdot\left(\boxed{23}-\boxed{17}\right) - \boxed{17} = 3\cdot\boxed{23} - 4\cdot\boxed{17}.$$

Hence, $-4\cdot 17 \equiv 1 \pmod{23}$. In other words, $17^{-1} \equiv -4 \pmod{23}$.

(b) Since $2\cdot 15 \equiv -1 \pmod{31}$, we see that $15^{-1} \equiv -2 \pmod{31}$.

(Don't worry if you didn't see that. You can just proceed as in the first part of this problem.)

Hence, $15x \equiv 7 \pmod{31}$ has the unique solution $x \equiv 15^{-1}\cdot 7 \equiv -2\cdot 7 \equiv 17 \pmod{31}$

(c) Recall that a residue $x$ is invertible modulo 10 if and only if $\gcd(x,10) = 1$.

Hence, the invertible residues modulo 10 are $1, 3, 7, 9$.

(d) This congruence has no solutions, because $\gcd(16,70) = 2$ but $2 \nmid 1$.

(e) Again $\gcd(16,70) = 2$, but this time $2|4$. Hence, we have $\gcd(16,70) = 2$ solutions modulo 70.

The congruence is equivalent to $8x \equiv 2 \pmod{35}$. We therefore determine $8^{-1} \pmod{35}$.

We use the extended Euclidean algorithm:

$$\begin{array}{rll} & \gcd(8,35) & \boxed{35} = 4\cdot\boxed{8}+3 \\ = & \gcd(3,8) & \boxed{8} = 3\cdot\boxed{3}-1 \\ = & 1 & \end{array}$$

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

$$1 = 3\cdot\boxed{3} - \boxed{8} = 3\cdot\left(\boxed{35}-4\cdot\boxed{8}\right) - \boxed{8} = 3\cdot\boxed{35} - 13\cdot\boxed{8}.$$

Hence, $8^{-1} \equiv -13 \pmod{35}$.

It follows that $8x \equiv 2 \pmod{35}$ has the unique solution $x \equiv 8^{-1}\cdot 2 \equiv -13\cdot 2 \equiv 9 \pmod{35}$.

Modulo 70, we have the two solutions $x \equiv 9 \pmod{70}$, $x \equiv 9+35 = 44 \pmod{70}$. □

**Problem 5.** Solve the following system of congruences:

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

(Use Homework Problems 2.14, 2.15 to generate more practice problems of this kind.)

**Solution.** Working with rational numbers, the system

$$\begin{array}{rcl} 3x+5y & = & 6 \\ 2x+7y & = & 2 \end{array}$$

has the unique solution (use any method you like)

$$\begin{bmatrix} x \\ y \end{bmatrix} = \begin{bmatrix} 3 & 5 \\ 2 & 7 \end{bmatrix}^{-1} \begin{bmatrix} 6 \\ 2 \end{bmatrix} = \frac{1}{11} \begin{bmatrix} 7 & -5 \\ -2 & 3 \end{bmatrix} \begin{bmatrix} 6 \\ 2 \end{bmatrix} = \frac{1}{11} \begin{bmatrix} 32 \\ -6 \end{bmatrix}.$$

Working modulo 25, we have to determine the modular inverse $11^{-1} \pmod{25}$.

Using the Euclidean algorithm, we find that $11x + 25y = 1$ is solved by $x = -9$, $y = 4$. (The steps are omitted here, since we are experts by now. Make sure you can do it, and don't omit the steps on the exam, unless there is an obvious choice for $x$ and $y$!) This shows that $11^{-1} \equiv -9 \pmod{25}$.

Hence, the system has the solution

$$\begin{bmatrix} x \\ y \end{bmatrix} \equiv 11^{-1} \begin{bmatrix} 32 \\ -6 \end{bmatrix} \equiv -9 \begin{bmatrix} 7 \\ -6 \end{bmatrix} \equiv \begin{bmatrix} 12 \\ 4 \end{bmatrix} \pmod{25}.$$

(Check by substituting the values into the two original congruences!) □

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

(a) Bézout's identity

(b) Prime number theorem

(c) Fermat's little theorem

**Solution.**

(a) Let $a, b \in \mathbb{Z}$ (not both zero). There exist $x, y \in \mathbb{Z}$ such that

$$\gcd(a, b) = ax + by.$$

(b) Let $\pi(x)$ be the number of primes $\leqslant x$. Then

$$\lim_{x \to \infty} \frac{\pi(x)}{x / \ln(x)} = 1.$$

(c) Let $p$ be a prime and $a$ an integer. If $p \nmid a$, then

$$a^{p-1} \equiv 1 \pmod{p}.$$ □

**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 the Euclidean algorithm.
- Using the previous part of this problem and binary exponentiation.

**Solution.**

(a) Recall that $x$ is a modular inverse of $a$ if and only if $ax \equiv 1 \pmod{n}$. This congruence has a solution $x$ if and only if the diophantine equation

$$ax + ny = 1$$

has a solution $x, y \in \mathbb{Z}$. This is the case if and only if $\gcd(a, n)$ divides the right-hand side, which is 1. That is the case if and only if $\gcd(a, n) = 1$.

(b) Since $p$ is a prime, and $a$ an integer such that $p \nmid a$, Fermat's little theorem states that

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

Equivalently, $a^{p-2} \cdot a \equiv 1 \pmod{p}$, which means that $a^{-1} \equiv a^{p-2} \pmod{p}$.

(c) We compute the modular inverse of 17 modulo 101 in two different ways:

- Using the Euclidean algorithm, we compute $\underbrace{\gcd(17, 101)}_{101 = 6 \cdot 17 - 1} = \gcd(1, 17) = 1$, so that Bézout's identity takes the simple form $1 = 6 \cdot 17 - 101$.

  Hence, $6 \cdot 17 \equiv 1 \pmod{101}$. In other words, $17^{-1} \equiv 6 \pmod{101}$.

- By the previous part of this problem,

  $$17^{-1} \equiv 17^{99} \pmod{101}.$$

  Note that $99 = 64 + 32 + 2 + 1$. Using binary exponentiation, we compute, modulo 101,

  $$17^2 \equiv -14, \quad 17^4 \equiv (-14)^2 \equiv -6, \quad 17^8 \equiv (-6)^2 \equiv 36, \quad 17^{16} \equiv 36^2 \equiv -17, \quad 17^{32} \equiv (-17)^2 \equiv -14,$$

  so that $17^{64} \equiv (-14)^2 \equiv -6$, repeating the initial values. Hence,

  $$17^{-1} \equiv 17^{99} = 17^{64} \cdot 17^{32} \cdot 17^2 \cdot 17^1 \equiv (-6) \cdot (-14) \cdot (-14) \cdot 17 \equiv 6 \pmod{101}.$$ □

**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 2.13 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 3.5 to generate more practice problems of this kind.)

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

(Use Homework Problem 3.6 to generate more practice problems of this kind.)

**Solution.**

(a) Since $\gcd(81,135)=27$, we have $\operatorname{lcm}(81,135)=\frac{81\cdot 135}{\gcd(81,135)}=\frac{81\cdot 135}{27}=405$.

(b) Modulo 6, we have $-2\equiv 4, -9\equiv 3, 6\equiv 0, 17\equiv 5, -10\equiv 2$. The missing residue is 1.

(c) $3141=523\cdot 6+3$. Hence, $3141=(...3)_6$ where ... are the digits for 523.

$523=87\cdot 6+1$. Hence, $3141=(...13)_6$ where ... are the digits for 87.

$87=14\cdot 6+3$. Hence, $3141=(...313)_6$ where ... are the digits for 14.

$14=2\cdot 6+2$. Hence, $3141=(...2313)_6$ where ... are the digits for 2.

In conclusion, $3141=(22313)_6$.

(d) $112358132134\equiv 1+1+2+3+5+8+1+3+2+1+3+4=34\equiv 7 \pmod 9$

The remainder of 112358132134 modulo 9 is 7.

(e) $62831853\equiv -6+2-8+3-1+8-5+3=-4\equiv 7 \pmod{11}$

The remainder of 62831853 modulo 11 is 7. □

**Problem 9.**

(a) Solve $x\equiv 2 \pmod{11}$, $x\equiv 3 \pmod{13}$.

(b) Using the Chinese remainder theorem, determine all solutions to $x^2\equiv 4 \pmod{55}$.

(Use Homework Problems 3.7, 3.8 to generate more practice problems of this kind.)

**Solution.**

(a) $x\equiv 2\cdot 13\cdot \underbrace{13^{-1}_{\bmod 11}}_{-5}+3\cdot 11\cdot \underbrace{11^{-1}_{\bmod 13}}_{6}\equiv -130+198\equiv 13+55\equiv 68 \pmod{143}$

**Comment.** Here, for instance, $11^{-1}\equiv -2^{-1}\equiv 6 \pmod{13}$ is easy to see with some practice (otherwise, we can always run the Euclidean algorithm).

(b) By the Chinese remainder theorem:

$$\begin{aligned} & x^2\equiv 4 \pmod{55} \\ \iff\ & x^2\equiv 4 \pmod 5 \text{ and } x^2\equiv 4 \pmod{11} \\ \iff\ & x\equiv \pm 2 \pmod 5 \text{ and } x\equiv \pm 2 \pmod{11} \end{aligned}$$

The two obvious solutions modulo 55 are $\pm 2$. To get one of the two additional solutions, we solve $x\equiv 2 \pmod 5$, $x\equiv -2 \pmod{11}$. [Then the other additional solution is the negative of that.]

$x\equiv 2\cdot 11\cdot \underbrace{11^{-1}_{\bmod 5}}_{1}-2\cdot 5\cdot \underbrace{5^{-1}_{\bmod 11}}_{-2}\equiv 22+20\equiv 42\equiv -13 \pmod{55}$

Hence, the solutions are $x\equiv \pm 2 \pmod{55}$ and $x\equiv \pm 13 \pmod{55}$. □