Midterm #1: practice

MATH 311 — Intro to Number Theory
Midterm: Thursday, Oct 4

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 1.1, 1.2, 1.3 to generate more practice problems of this kind.)

Solution. The gcd is

$$d = \underbrace{\gcd(119, 272)}_{272 = 2 \cdot 119 + 34} = \underbrace{\gcd(34, 119)}_{119 = 3 \cdot 34 + 17} = \gcd(17, 34) = 17.$$

We trace back through the Euclidean algorithm to find integers x, y such that $119x + 272y = 17$:

$$17 = \underbrace{119 - 3 \cdot 34}_{34 = 272 - 2 \cdot 119} = 7 \cdot 119 - 3 \cdot 272$$

So, here, $x = 7$ and $y = -3$.

Comment. Note that other values also work for x and y. In fact, the general solution is $x = 7 + \frac{272}{17}t$, $y = -3 - \frac{119}{17}t$. □

Problem 2.

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

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

(Use Homework Problems 1.7, 1.8 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 $41x + 120y = 33$.

We already know that $\gcd(41, 120) = 1$ but to find integers x, y such that $41x + 120y = 1$, we go through the Euclidean algorithm again (if you want, you could reuse our previous computation; note that everything is the same just with the common factor of 3 cancelled everywhere):

$$\underbrace{\gcd(41, 120)}_{120 = 2 \cdot 41 + 38} = \underbrace{\gcd(38, 41)}_{41 = 1 \cdot 38 + 3} = \underbrace{\gcd(3, 38)}_{38 = 12 \cdot 3 + 2} = \underbrace{\gcd(2, 3)}_{3 = 1 \cdot 2 + 1} = \gcd(1, 2) = 1.$$

We trace back through the algorithm to find

$$1 = \underbrace{3 - 1 \cdot 2}_{2 = 38 - 12 \cdot 3} = \underbrace{-1 \cdot 38 + 13 \cdot 3}_{3 = 41 - 1 \cdot 38} = \underbrace{13 \cdot 41 - 14 \cdot 38}_{38 = 120 - 2 \cdot 41} = -14 \cdot 120 + 41 \cdot 41.$$

In other words, $41x + 120y = 1$ has the solution $x = 41$, $y = -14$.

Multiplying this equation with 33, we find that our original equation $41x + 120y = 33$ has the particular solution $x = 33 \cdot 41$, $y = -33 \cdot 14$.

The general solution is $x = 33 \cdot 41 + 120t$, $y = -33 \cdot 14 - 41t$ with t any integer.

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

Armin Straub
straub@southalabama.edu

Problem 3.

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

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

(c) 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) Before we start using binary exponentiation, we should simplify $31^{41} \equiv 8^{41} = 8^{22} \cdot 8^{19} \equiv 8^{19} \pmod{23}$.

$8^2 = 64 \equiv -5 \pmod{23}$, $8^4 \equiv (-5)^2 \equiv 2$, $8^8 \equiv 2^2 = 4$, $8^{16} \equiv 4^2 = 16$.

Hence, $31^{41} \equiv 8^{19} = 8^{16} \cdot 8^2 \cdot 8^1 \equiv 16 \cdot \underbrace{(-5) \cdot 8}_{\equiv 6} \equiv 4 \pmod{23}$.

(b) 41 is a prime. Hence, by Fermat's little theorem, $a^{41} \equiv a \pmod{41}$ for any integer a. So, $31^{41} \equiv 31 \pmod{41}$.

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

Note that 19 is a prime. Therefore, for any integer a such that $a \not\equiv 0 \pmod{19}$, we have $a^{18} \equiv 1 \pmod{19}$ by Fermat's little theorem. We can therefore use $159 \equiv 15 \pmod{18}$ to simplify

$$10^{159} \equiv 10^{15} \pmod{19}.$$

We 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 2.6, 2.7, 2.8, 2.9 to generate more practice problems of this kind.)

Solution.

(a) We use the extended Euclidean algorithm: $\underbrace{\gcd(17, 23)}_{23 = 1 \cdot 17 + 6} = \underbrace{\gcd(6, 17)}_{17 = 3 \cdot 6 - 1} = \gcd(1, 6) = 1$

Hence, Bézout's identity takes the form $1 = \underbrace{3 \cdot 6 - 17}_{6 = 23 - 1 \cdot 17} = 3 \cdot 23 - 4 \cdot 17$.

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 $1, 3, 7, 9$.

Armin Straub
straub@southalabama.edu

(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: $\underbrace{\gcd(8,35)}_{35=4\cdot 8+3}=\underbrace{\gcd(3,8)}_{8=3\cdot 3-1}=\gcd(1,3)=1$

Hence, Bézout's identity takes the form $1=\underbrace{3\cdot 3-8}_{3=35-4\cdot 8}=3\cdot 35-13\cdot 8$.

Hence, $-13\cdot 8\equiv 1 \pmod{35}$. In other words, $8^{-1}\equiv -13 \pmod{35}$.

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:

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

(Use Homework Problems 2.10, 2.11 to generate more practice problems of this kind.)

Solution. Working with rational numbers, the system

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

has 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) Fermat's little theorem

Solution.

(a) Bézout's identity:

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

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

(b) Fermat's little theorem:

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 Bézout's identity.
- 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 simply takes the 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 $99 = 64 + 32 + 2 + 1$. 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 $\operatorname{lcm}(81, 135)$.

Armin Straub
straub@southalabama.edu

(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 2.5 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 2.6 to generate more practice problems of this kind.)

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

(Use Homework Problem 2.7 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. We call (a, b, c) a prime triple if a, b, c are all primes.

(a) List the first few prime triples of the form $(p, p + 2, p + 6)$.
(It is believed, but nobody can show, that there are infinitely many such triples.)

(b) Show that there is only a single prime triple of the form $(p, p + 2, p + 4)$.

(c) Show that there are no prime triples of the form $(p, p + 2, p + 5)$.

Solution.

(a) $(5, 7, 11)$, $(11, 13, 17)$, $(17, 19, 23)$, $(41, 43, 47)$, $(101, 103, 107)$, ...

(b) For any integer x, one of the integers x, $x + 2$, $x + 4$ is divisible by 3 (because $x + 4 \equiv x + 1 \pmod{3}$). Hence, in each triple $(p, p + 2, p + 4)$, one of the three numbers is divisible by 3.

This leaves $p = 3$ as the only possibility and, indeed, $(3, 5, 7)$ is a prime triple.

(c) Either p or $p + 5$ is an even number, and hence divisible by 2.

This leaves $p = 2$ as the only possibility, but $(2, 4, 7)$ is not a prime triple. □