Midterm #2: practice

MATH 311 — Intro to Number Theory
midterm: Thursday, Oct 20

Please print your name:

Calculators will not be permitted on the exam. The numbers on the exam will be suitable for calculating by hand.

Problem 1.

(a) Express 3141 in base 6.

(b) Determine, without the help of a calculator, the remainder of 112358132134 modulo 9.

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

(d) Is $0, 1, 2, 4, 8, \ldots, 2^{11}$ a complete set of residues modulo 13?

(e) Is 2 a primitive root modulo 11? What about 3?

Do you see a way to determine all primitive roots modulo 11 without much further computation?

Solution.

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

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

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

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

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

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

The remainder of 112358132134 modulo 9 is 7.

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

The remainder of 62831853 modulo 11 is 7.

(d) $2^0 = 1,\ 2^1 = 2,\ 2^2 = 4,\ 2^3 = 8,\ 2^4 = 16 \equiv 3,\ 2^5 \equiv 2 \cdot 3 = 6,\ 2^6 \equiv 2 \cdot 6 = 12 \equiv -1$

The values now repeat with a minus sign: $2^7 = 2^6 \cdot 2^1 \equiv -2 \equiv 11$, $2^8 \equiv -4 \equiv 9$, $2^9 \equiv -8 \equiv 5$, $2^{10} \equiv -3 \equiv 10$, $2^{11} \equiv -6 \equiv 7$.

Hence, the values $0, 1, 2, 4, 8, \ldots, 2^{11}$ are congruent, modulo 13, to $0, 1, 2, 4, 8, 3, 6, 12, 11, 9, 5, 10, 7$. So, indeed, they form a complete set of residues modulo 13.

(e) $2^0 = 1, 2^1 = 2, 2^2 = 4, 2^3 = 8, 2^4 \equiv 5, 2^5 \equiv 2 \cdot 5 = 10, 2^6 \equiv 2 \cdot 10 \equiv 9, 2^7 \equiv 2 \cdot 9 \equiv 7, 2^8 \equiv 2 \cdot 7 \equiv 3, 2^9 \equiv 2 \cdot 3 = 6, 2^{10} \equiv 2 \cdot 6 \equiv 1$

Hence, 2 is a primitive root modulo 11.

On the other hand, $3 \equiv 2^8$ is not a primitive root because $3^5 \equiv 2^{40} = (2^{10})^4 \equiv 1 \pmod{11}$.

If you think about this argument, you will see that 2^a is a primitive root modulo 11 if and only if $\gcd(a, 10) = 1$. Hence, the primitive roots modulo 11 are $2^1 = 2$, $2^3 = 8$, $2^7 \equiv 7$, $2^9 \equiv 6$. □

Problem 2.

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

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

(c) Show that $314^{159} + 265^{358} + 10$ is divisible by 19.

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 $314^{159} + 265^{358} + 10 \equiv 10^{15} + 11 \equiv 8 + 11 \equiv 0 \pmod{19}$.

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

Problem 3.

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

(b) Solve $15x \equiv 7 \pmod{31}$.

(c) How many solutions does $16x \equiv 1 \pmod{70}$ have modulo 70? Find all solutions.

(d) How many solutions does $16x \equiv 4 \pmod{70}$ have modulo 70? Find all solutions.

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

(d) Again $\gcd(16, 70) = 2$, but this time $2|4$. Hence, we have 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 $1 = \underbrace{3}_{3=35-4\cdot 8} \cdot 3 - 8 = 3 \cdot 35 - 13 \cdot 8$.

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 4. Solve the following system of congruences:

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

Solution. Working with rational numbers, the system

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

has solution (use any method you like)

$$\left[\begin{array}{c} x \\ y \end{array}\right] = \left[\begin{array}{cc} 3 & 5 \\ 2 & 7 \end{array}\right]^{-1} \left[\begin{array}{c} 6 \\ 2 \end{array}\right] = \frac{1}{11} \left[\begin{array}{cc} 7 & -5 \\ -2 & 3 \end{array}\right] \left[\begin{array}{c} 6 \\ 2 \end{array}\right] = \frac{1}{11} \left[\begin{array}{c} 32 \\ -6 \end{array}\right].$$

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

Using the Euclidian 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

$$\left[\begin{array}{c} x \\ y \end{array}\right] \equiv 11^{-1} \left[\begin{array}{c} 32 \\ -6 \end{array}\right] \equiv -9 \left[\begin{array}{c} 7 \\ -6 \end{array}\right] \equiv \left[\begin{array}{c} 12 \\ 4 \end{array}\right] \pmod{25}.$$

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

Problem 5.

(a) Solve $x \equiv 1 \pmod{3}$, $x \equiv 2 \pmod{4}$, $x \equiv 3 \pmod{5}$, $x \equiv 4 \pmod{11}$.

(b) Solve $x \equiv 1 \pmod{3}$, $x \equiv 2 \pmod{4}$, $2x \equiv 3 \pmod{5}$, $3x \equiv 4 \pmod{11}$.

(c) Find the smallest integer $a > 2$ such that $2|a$, $3|(a+1)$, $4|(a+2)$ and $5|(a+3)$.

Solution.

(a) We break the problem into four pieces:

- $x \equiv 1 \pmod{3}$, $x \equiv 0 \pmod{4}$, $x \equiv 0 \pmod{5}$, $x \equiv 0 \pmod{11}$.

  To satisfy the mod 4, mod 5 and mod 11 congruences, we need $x = 4 \cdot 5 \cdot 11z$.

  We solve $4 \cdot 5 \cdot 11z \equiv 1 \pmod{3}$. Simplifies to $z \equiv 1 \pmod{3}$. $z = 1$ gives $x = 4 \cdot 5 \cdot 11 = 220$.

- $x \equiv 0 \pmod{3}$, $x \equiv 1 \pmod{4}$, $x \equiv 0 \pmod{5}$, $x \equiv 0 \pmod{11}$. We need $x = 3 \cdot 5 \cdot 11z$.

  Solving $3 \cdot 5 \cdot 11z \equiv 1 \pmod{4}$. Simplifies to $z \equiv 1 \pmod{4}$. $z = 1$ gives $x = 3 \cdot 5 \cdot 11 = 165$.

- $x \equiv 0 \pmod{3}$, $x \equiv 0 \pmod{4}$, $x \equiv 1 \pmod{5}$, $x \equiv 0 \pmod{11}$. We need $x = 3 \cdot 4 \cdot 11z$.

  Solving $3 \cdot 4 \cdot 11z \equiv 1 \pmod{5}$. Simplifies to $2z \equiv 1 \pmod{5}$, which has solution $z \equiv 3 \pmod{5}$.

  $z = 3$ gives $x = 3 \cdot 4 \cdot 11 \cdot 3 = 396$.

- $x \equiv 0 \pmod{3}$, $x \equiv 0 \pmod{4}$, $x \equiv 0 \pmod{5}$, $x \equiv 1 \pmod{11}$. We need $x = 3 \cdot 4 \cdot 5z$.

  Solving $3 \cdot 4 \cdot 5z \equiv 1 \pmod{11}$. Simplifies to $5z \equiv 1 \pmod{11}$, which has solution $z \equiv -2 \pmod{11}$.

  $z = -2$ gives $x = 3 \cdot 4 \cdot 5 \cdot (-2) = -120$.

Combining these four, $x \equiv 1 \pmod{3}$, $x \equiv 2 \pmod{4}$, $x \equiv 3 \pmod{5}$, $x \equiv 4 \pmod{11}$ has solution

$x = 1 \cdot 220 + 2 \cdot 165 + 3 \cdot 396 + 4 \cdot (-120) = 1258$.

Since $3 \cdot 4 \cdot 5 \cdot 11 = 660$, the general solution is $x \equiv 1308 \equiv -62 \pmod{660}$ by the Chinese remainder theorem.

(b) $2x \equiv 3 \pmod{5}$ has the unique solution $x \equiv 2^{-1} \cdot 3 \equiv 3 \cdot 3 \equiv -1 \pmod{5}$.

$3x \equiv 4 \pmod{11}$ has the unique solution $x \equiv 3^{-1} \cdot 4 \equiv 4 \cdot 4 \equiv 5 \pmod{11}$.

Our simplified task is to solve $x \equiv 1 \pmod{3}$, $x \equiv 2 \pmod{4}$, $x \equiv -1 \pmod{5}$, $x \equiv 5 \pmod{11}$. We reuse the previous part to produce the solution $x = 1 \cdot 220 + 2 \cdot 165 - 1 \cdot 396 + 5 \cdot (-120) = -446$.

Therefore, the general solution is $x \equiv -446 \equiv 214 \pmod{660}$ by the Chinese remainder theorem.

(c) This is the same as solving $a \equiv 0 \pmod{2}$, $a \equiv -1 \pmod{3}$, $a \equiv -2 \pmod{4}$, $a \equiv -3 \pmod{5}$. Notice that we can't apply the Chinese remainder theorem directly, because 2 and 4 are not coprime.

However, if $a \equiv -2 \pmod{4}$ then, automatically, $a \equiv 0 \pmod{2}$. So, we can drop the latter congruence and only look for solutions of $a \equiv -1 \pmod{3}$, $a \equiv -2 \pmod{4}$, $a \equiv -3 \pmod{5}$.

By the Chinese remainder theorem (since 3, 4, 5 are pairwise coprime), there is a unique solution a modulo $3 \cdot 4 \cdot 5 = 60$. Note that $a = 2$ is such a solution. Hence, the next smallest solution is $a = 62$.

[No problem if you didn't see that $a = 2$ is a solution. You can find it by going through the same kind of computations as in the previous parts.] □

— There is two more problems on the second page... —

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

(a) Bézout's identity

(b) Fermat's little theorem

(c) Chinese remainder 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 suppose that $p \nmid a$. Then

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

(c) Chinese remainder theorem:

Let $n_1, n_2, \ldots, n_r$ be positive integers with $\gcd(n_i, n_j) = 1$ for $i \neq j$. Then the system of congruences

$$x \equiv a_1 \ (\mathrm{mod}\, n_1), \quad \ldots, \quad x \equiv a_n \ (\mathrm{mod}\, n_r)$$

has a simultaneous solution, which is unique modulo $n = n_1 \cdots n_r$. □

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 the modular inverse of 17 modulo 101 in two different ways:

- Using the previous part of this problem, and binary exponentiation.
- Using Bézout's identity.

Solution.

(a) Recall that x is a modular inverse of a if and only if $ax \equiv 1 \ (\mathrm{mod}\, n)$. 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:

- 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,

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

- Using the Euclidian 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, $17^{-1} \equiv 6 \pmod{101}$. □

— It is also a very good idea to review the problems from Homework 4. —