MATH 433

Applied Algebra

Lecture 8:
Review for Exam 1.

Topics for Exam 1

- Greatest common divisor, Euclidean algorithm
- Primes, factorisation, Unique Factorisation Theorem
- Congruence classes, modular arithmetic
- Inverse of a congruence class
- Linear congruences
- Chinese Remainder Theorem
- Order of a congruence class
- Fermat's litle theorem, Euler's theorem
- Euler's totient function
- Public key encryption, the RSA system

- Mathematical induction
- Relations

Sample problems

Problem 1. Find $\gcd(1106, 350)$.

Problem 2. Find an integer solution of the equation $45x + 115y = 10$.

Problem 3. Prove by induction that

$$\frac{1}{4} + \frac{1}{16} + \cdots + \frac{1}{4^n} = \frac{1}{3}\left(1 - \frac{1}{4^n}\right)$$

for every positive integer n.

Problem 4. When the number $14^7 \cdot 25^{30} \cdot 40^{12}$ is written out, how many zeroes are there at the right-hand end?

Problem 5. Find a multiplicative inverse of 29 modulo 41.

Problem 6. Which congruence classes modulo 8 are invertible?

Problem 7. Find an integer x such that $21x \equiv 5 \bmod 31$.

Sample problems

Problem 8. Solve the system $\begin{cases} y \equiv 4 \bmod 7, \\ y \equiv 5 \bmod 11. \end{cases}$

Problem 9. Find the multiplicative order of 7 modulo 36.

Problem 10. Determine the last two digits of 7^{303}.

Problem 11. How many integers from 1 to 120 are relatively prime with 120?

Problem 12. You receive a message that was encrypted using the RSA system with public key $(33, 7)$, where 33 is the base and 7 is the exponent. The encrypted message, in two blocks, is $5/31$. Find the private key and decrypt the message.

Problem 13. Let R be the relation defined on the set of positive integers by xRy if and only if $\gcd(x, y) \neq 1$ ("is not coprime with"). Is this relation reflexive? Symmetric? Transitive?

Problem 1. Find $\gcd(1106, 350)$.

To find the greatest common divisor of 1106 and 350, we apply the Euclidean algorithm to these numbers.

First we divide 1106 by 350: $1106 = 350 \cdot 3 + 56$,
next we divide 350 by 56: $350 = 56 \cdot 6 + 14$,
next we divide 56 by 14: $56 = 14 \cdot 4$.

It follows that $\gcd(1106, 350) = \gcd(350, 56) = \gcd(56, 14) = 14$.

Alternatively, we could use the Euclidean algorithm in matrix form:

$$\left(\begin{array}{cc|c} 1 & 0 & 1106 \\ 0 & 1 & 350 \end{array}\right) \to \left(\begin{array}{cc|c} 1 & -3 & 56 \\ 0 & 1 & 350 \end{array}\right) \to \left(\begin{array}{cc|c} 1 & -3 & 56 \\ -6 & 19 & 14 \end{array}\right)$$

$$\to \left(\begin{array}{cc|c} 25 & -79 & 0 \\ -6 & 19 & 14 \end{array}\right).$$

Now $\gcd(1106, 350)$ is the nonzero entry in the rightmost column of the last matrix, which is 14.

Problem 2. Find an integer solution of the equation $45x + 115y = 10$.

First we use the Euclidean algorithm to find $\gcd(45, 115)$ and represent it as an integral linear combination of 45 and 115:

$$\left(\begin{array}{cc|c} 1 & 0 & 45 \\ 0 & 1 & 115 \end{array}\right) \to \left(\begin{array}{cc|c} 1 & 0 & 45 \\ -2 & 1 & 25 \end{array}\right) \to \left(\begin{array}{cc|c} 3 & -1 & 20 \\ -2 & 1 & 25 \end{array}\right)$$

$$\to \left(\begin{array}{cc|c} 3 & -1 & 20 \\ -5 & 2 & 5 \end{array}\right) \to \left(\begin{array}{cc|c} 23 & -9 & 0 \\ -5 & 2 & 5 \end{array}\right).$$

It follows that $\gcd(45, 115) = 5$. Also, from the second row of the last matrix we read off that $(-5) \cdot 45 + 2 \cdot 115 = 5$.

Multiplying both sides by 2, we get that $x = -10$, $y = 4$ is a solution.

Problem 3. Prove by induction that

$$\frac{1}{4}+\frac{1}{16}+\cdots+\frac{1}{4^n}=\frac{1}{3}\left(1-\frac{1}{4^n}\right)$$

for every positive integer n.

The proof is by induction on n. First consider the case $n=1$. In this case the formula reduces to $\frac{1}{4}=\frac{1}{3}\left(1-\frac{1}{4}\right)$, which is a true equality.

Now assume that the formula holds for $n=k$, that is,

$$\tfrac{1}{4}+\tfrac{1}{16}+\cdots+\tfrac{1}{4^k}=\tfrac{1}{3}\left(1-\tfrac{1}{4^k}\right).$$

Then $\frac{1}{4}+\frac{1}{16}+\cdots+\frac{1}{4^k}+\frac{1}{4^{k+1}}=\frac{1}{3}\left(1-\frac{1}{4^k}\right)+\frac{1}{4^{k+1}}$
$=\frac{1}{3}-\frac{1}{3}\cdot\frac{1}{4^k}+\frac{1}{4}\cdot\frac{1}{4^k}=\frac{1}{3}-\frac{1}{12}\cdot\frac{1}{4^k}=\frac{1}{3}\left(1-\frac{1}{4^{k+1}}\right)$,
which means that the formula holds for $n=k+1$ as well.

By induction, the formula holds for every positive integer n.

Problem 4. When the number $14^7 \cdot 25^{30} \cdot 40^{12}$ is written out, how many zeroes are there at the right-hand end?

The number of consecutive zeroes at the right-hand end is the exponent of the largest power of 10 that divides our number.

The prime factorisation of the given number is

$$14^7 \cdot 25^{30} \cdot 40^{12} = (2 \cdot 7)^7 \cdot (5^2)^{30} \cdot (2^3 \cdot 5)^{12} = 2^{73} \cdot 5^{72} \cdot 7^7.$$

For any integer $n > 0$ the prime factorisation of 10^n is $2^n \cdot 5^n$.

As follows from the Unique Factorisation Theorem, a positive integer A divides another positive integer B if and only if the prime factorisation of A is part of the prime factorisation of B.

Hence 10^n divides the given number if $n \leq 73$ and $n \leq 72$. The largest number with this property is 72. Thus there are 72 zeroes at the right-hand end.

Problem 5. Find a multiplicative inverse of 29 modulo 41.

To find the inverse, we need to represent 1 as an integral linear combination of 29 and 41. Let us apply the Euclidean algorithm (in matrix form) to 29 and 41:

$$\left(\begin{array}{cc|c} 1 & 0 & 29 \\ 0 & 1 & 41 \end{array}\right) \to \left(\begin{array}{cc|c} 1 & 0 & 29 \\ -1 & 1 & 12 \end{array}\right) \to \left(\begin{array}{cc|c} 3 & -2 & 5 \\ -1 & 1 & 12 \end{array}\right)$$

$$\to \left(\begin{array}{cc|c} 3 & -2 & 5 \\ -7 & 5 & 2 \end{array}\right) \to \left(\begin{array}{cc|c} 17 & -12 & 1 \\ -7 & 5 & 2 \end{array}\right).$$

From the first row of the last matrix we read off that $17 \cdot 29 - 12 \cdot 41 = 1$. Hence $17 \cdot 29 \equiv 1 \bmod 41$.

It follows that $[17]_{41}[29]_{41} = [1]_{41}$, which means that $[29]_{41}^{-1} = [17]_{41}$. Thus 17 is the inverse of 29 modulo 41.

Problem 6. Which congruence classes modulo 8 are invertible?

A congruence class $[a]_n$ is invertible if and only if a is coprime with n.

There are 8 congruence classes modulo 8:

$$[0], [1], [2], [3], [4], [5], [6], [7].$$

The congruence classes of even numbers are not invertible. The classes of odd numbers are invertible.

$[1]^{-1} = 1,\ [3]^{-1} = [3],\ [5]^{-1} = [5],\ [7]^{-1} = [7].$

Every invertible class is its own inverse.

Problem 7. Find an integer x such that $21x \equiv 5 \bmod 31$.

To solve this linear congruence, we need to find the inverse of 21 modulo 31. For this, we need to represent 1 as an integral linear combination of 21 and 31. This can be done either by inspection or by the matrix method:

$$\left(\begin{array}{cc|c} 1 & 0 & 21 \\ 0 & 1 & 31 \end{array}\right) \to \left(\begin{array}{cc|c} 1 & 0 & 21 \\ -1 & 1 & 10 \end{array}\right) \to \left(\begin{array}{cc|c} 3 & -2 & 1 \\ -1 & 1 & 10 \end{array}\right).$$

From the first row we read off that $3 \cdot 21 - 2 \cdot 31 = 1$, which implies that 3 is the inverse of 21 modulo 31.

Thus $21x \equiv 5 \bmod 31 \iff x \equiv 3 \cdot 5 \bmod 31$
$\iff x \equiv 15 \bmod 31$.

In alternative notation (with congruence classes modulo 31),

$$[21][x] = [5] \iff [x] = [21]^{-1}[5] = [3][5] = [15].$$

Problem 8. Solve the system $\begin{cases} y \equiv 4 \bmod 7, \\ y \equiv 5 \bmod 11. \end{cases}$

The moduli 7 and 11 are coprime. First we use the Euclidean algorithm to represent 1 as an integral linear combination of 7 and 11:

$$\left(\begin{array}{cc|c} 1 & 0 & 7 \\ 0 & 1 & 11 \end{array}\right) \to \left(\begin{array}{cc|c} 1 & 0 & 7 \\ -1 & 1 & 4 \end{array}\right) \to \left(\begin{array}{cc|c} 2 & -1 & 3 \\ -1 & 1 & 4 \end{array}\right)$$
$$\to \left(\begin{array}{cc|c} 2 & -1 & 3 \\ -3 & 2 & 1 \end{array}\right).$$

Hence $(-3) \cdot 7 + 2 \cdot 11 = 1$. Then one of the solutions is $y = 5(-3) \cdot 7 + 4 \cdot 2 \cdot 11 = -17$.

The general solution is $y \equiv -17 \bmod 77$.

Problem 8. Solve the system $\begin{cases} y \equiv 4 \bmod 7, \\ y \equiv 5 \bmod 11. \end{cases}$

Alternative solution: From the second congruence we find that $y = 5 + 11k$, where k is an integer. Substituting this into the first congruence, we obtain

$$5 + 11k \equiv 4 \bmod 7 \iff 11k \equiv -1 \bmod 7$$
$$\iff 4k \equiv -1 \bmod 7.$$

Multiplying both sides of the last congruence by 2 (which is the inverse of 4 modulo 7), we get

$$8k \equiv -2 \bmod 7 \iff k \equiv -2 \bmod 7.$$

Thus $k = -2 + 7s$, where s is an integer. Then
$y = 5 + 11k = 5 + 11(-2 + 7s) = -17 + 77s$.

Problem 9. Find the multiplicative order of 7 modulo 36.

The multiplicative order of 7 modulo 36 is the smallest positive integer n such that $7^n \equiv 1 \bmod 36$ (it is well defined since 7 is coprime with 36). As follows from Euler's theorem, the order divides

$$\phi(36) = \phi(2^2 \cdot 3^2) = \phi(2^2)\phi(3^2) = (2^2 - 2)(3^2 - 3) = 12.$$

To find the order, we compute consecutive powers of the congruence class of 7 modulo 36:

$[7]^2 = [49] = [13]$,
$[7]^3 = [7]^2[7] = [13][7] = [91] = [19]$,
$[7]^4 = ([7]^2)^2 = [13]^2 = [169] = [25] = [-11]$,
since 5 does not divide 12, there is no need to compute $[7]^5$,
$[7]^6 = [7]^4[7]^2 = [-11][13] = [-143] = [1]$.

Thus the order of 7 modulo 36 is 6.

Remark. In the case $[7]^6 \neq [1]$, we would conclude that the order is 12.

Problem 10. Determine the last two digits of 7^{303}.

The last two digits are the remainder under division by 100. Since $\phi(100) = \phi(2^2 \cdot 5^2) = (2^2 - 2)(5^2 - 5) = 40$, we have $7^{40} \equiv 1 \bmod 100$ due to Euler's theorem. Then

$$[7^{303}] = [7]^{303} = [7]^{40\cdot 7+23} = ([7]^{40})^7\,[7]^{23} = [7]^{23}.$$

To simplify computation, we use the Chinese Remainder Theorem, which says that a congruence class $[a]_{100}$ is uniquely determined by the congruence classes $[a]_4$ and $[a]_{25}$.

Since $\phi(4) = \phi(2^2) = 2$ and $\phi(25) = \phi(5^2) = 20$, it follows from Euler's theorem that $7^2 \equiv 1 \bmod 4$ and $7^{20} \equiv 1 \bmod 25$.

Then $[7]_4^{23} = [7]_4 = [3]_4$ and $[7]_{25}^{23} = [7]_{25}^3 = [49]_{25}[7]_{25}$
$= [-1]_{25}[7]_{25} = [-7]_{25} = [18]_{25}$.

Since $7^{303} \equiv 7^{23} \equiv 18 \bmod 25$, the remainder of 7^{303} under division by 100 is among the four numbers 18, $43 = 18 + 25$, $68 = 18 + 25 \cdot 2$, and $93 = 18 + 25 \cdot 3$. We pick the one that has remainder 3 under division by 4. That's 43.

Problem 11. How many integers from 1 to 120 are relatively prime with 120?

The number of integers from 1 to n that are relatively prime with n is given by Euler's totient function $\phi(n)$.

To find $\phi(120)$, we expand 120 into a product of primes:

$$120 = 10 \cdot 12 = 2 \cdot 5 \cdot 4 \cdot 3 = 2^3 \cdot 3 \cdot 5.$$

Then

$$\phi(120) = \phi(2^3)\,\phi(3)\,\phi(5) = (2^3 - 2^2)(3-1)(5-1) = 32.$$

Problem 12. You receive a message that was encrypted using the RSA system with public key $(33, 7)$, where 33 is the base and 7 is the exponent. The encrypted message, in two blocks, is $5/31$. Find the private key and decrypt the message.

First we find that $\phi(33) = \phi(3)\phi(11) = (3-1)(11-1) = 20$.

The private key is $(33, \beta)$, where the exponent β is the inverse of 7 (the exponent from the public key) modulo $\phi(33) = 20$. It is easy to find by inspection that $\beta = 3$ (as $3 \cdot 7 = 21 \equiv 1 \bmod 20$). Clearly, this could also be done by applying the Euclidean algorithm to 7 and 20.

Now that we know the private key, the decrypted message is b_1/b_2, where $b_1 \equiv 5^3 \bmod 33$, $b_2 \equiv 31^3 \bmod 33$, and $0 \leq b_1, b_2 < 33$. We find that

$$[b_1]_{33} = [5]_{33}^3 = [5^3]_{33} = [125]_{33} = [26]_{33},$$
$$[b_2]_{33} = [31]_{33}^3 = [-2]_{33}^3 = [(-2)^3]_{33} = [-8]_{33} = [25]_{33}.$$

Thus the decrypted message is $26/25$.

Problem 13. Let R be the relation defined on the set $\mathbb{P}$ of positive integers by xRy if and only if $\gcd(x, y) \neq 1$ ("is not coprime with"). Is this relation reflexive? Symmetric? Transitive?

The relation R is not reflexive since 1 is not related to itself (actually, this is the only positive integer not related to itself by R).

The relation is symmetric since $\gcd(x, y) = \gcd(y, x)$ for all $x, y \in \mathbb{P}$.

The relation is not transitive as the following counterexample shows: $2R6$ and $6R3$, but 2 is not related to 3 by R.