

MATH 301, Section A01

Name _____ Solutions _____

Summer, 2011

Exam 3

Student ID number _____

PART A. (8 points each) *Carefully* define each of the following terms. Use complete sentences. Give only the definition of the defined term, not related concepts or examples.

1. Pseudoprime to the base b where b is a positive integer.

A positive integer n is a pseudoprime to the base b if n is composite and $b^n \equiv b \pmod{n}$.

2. Euler's theorem.

If a and n are integers such that $n \geq 2$ and $\gcd(a, n) = 1$, then $a^{\varphi(n)} \equiv 1 \pmod{n}$.

3. Quadratic residue \pmod{m} where $m \in \mathbb{Z}$, $m \geq 2$.

The integer a is a quadratic residue \pmod{m} if $\gcd(a, m) = 1$ and there is an integer x such that $x^2 \equiv a \pmod{m}$.

4. The Legendre symbol $\left(\frac{a}{m}\right)$, where a and m are relatively prime integers and $m \geq 2$.

$$\left(\frac{a}{m}\right) = \begin{cases} 1 & \text{If } a \text{ is a quadratic residue of } m. \\ -1 & \text{If } a \text{ is a quadratic nonresidue of } m. \end{cases}$$

5. The Law of Quadratic Reciprocity

If p and q are distinct odd primes, then $\left(\frac{p}{q}\right) = \left(\frac{q}{p}\right) (-1)^{\left(\frac{p-1}{2}\right)\left(\frac{q-1}{2}\right)}$.

PART B. (12 points each) *Carefully* do five of the following six problems. Mark clearly the problem which you do not want graded, and put in the box below the number of the problem that you do not want graded:

Problem which you don't want graded:

1. Let $n = 40500 = 2^2 \cdot 5^3 \cdot 3^4$.

(a) Find $\varphi(n)$. Be sure to show your work.

$$\varphi(n) = (2^2 - 2)(5^3 - 5^2)(3^4 - 3^3) = 2(100)(54) = 10800.$$

Answer:

10800

(b) Find $\sigma(n)$. Be sure to show your work.

$$\sigma(n) = \left(\frac{2^3-1}{2-1}\right) \left(\frac{5^4-1}{5-1}\right) \left(\frac{3^5-1}{3-1}\right) = 7(156)(121) = 132132.$$

Answer:

132132

2. Use Euler's Theorem to find the remainder when $2^{1600000047}$ is divided by 55.

Since $55 = 5 \cdot 11$, $\varphi(55) = \varphi(5)\varphi(11) = 4 \cdot 10 = 40$. By Euler's Theorem, $2^{40} \equiv 1 \pmod{55}$. Since $1600000047 \equiv 47 \equiv 7 \pmod{40}$, there is a $k \in \mathbb{Z}^+$ such that $1600000047 = 40k + 7$, so $2^{1600000047} = 2^{40k} 2^7 \equiv 2^7 \equiv 128 \equiv 18 \pmod{55}$. Therefore, the remainder is 18.

Answer:

18

3. The following message was encoded using the three level zigzag method.
Decode the message.

WEXNSEEDAEOAENTSX

The message has 17 characters. We put the first 5 characters in the positions which are congruent to 0 mod 4.

W--E--X--N--S

We then put the next 8 letters in the positions which are congruent to 1 or 3 mod 4.

WE-EED-AXE-ONA-ES

Finally, we put the last 4 letters in the remaining places.

WENEEDTAXESONAXES

Inserting spaces gives:

WE NEED TAXES ON AXES

Answer:

WE NEED TAXES ON AXES.

Problems 4 and 5 refer to the following situation.

A primitive alphabet has only letters A, B, C, and D with numerical values given by

A	B	C	D
01	02	03	04

An RSA scheme uses $n = 55$ and $e = 7$.

4. Encode the message consisting of the single letter C.

We need to compute $(03)^7 \pmod{55}$.

$$\begin{aligned} 3^7 &\equiv 3^4 \cdot 3^3 \pmod{55} \\ &\equiv (81)(27) \pmod{55} \\ &\equiv (26)(27) \pmod{55} \\ &\equiv (78)(9) \pmod{55} \\ &\equiv (23)(9) \pmod{55} \\ &\equiv (69)(3) \pmod{55} \\ &\equiv (14)(3) \pmod{55} \\ &\equiv 42 \pmod{55} \end{aligned}$$

Answer:

42

5. To which exponent should the coded block 49 be raised in order to decode the block? Express your answer as a non-negative integer.

Since the prime factorization of n is $(5)(11)$, and $(5-1)(11-1) = 40$, we need an inverse \bar{e} of $e = 7 \pmod{40}$. We must solve the diophantine equation $7x + 40y = 1$. Using the Euclidean algorithm we get

$$40 = 5 \cdot 7 + 5.$$

$$7 = 5 \cdot 1 + 2.$$

$$5 = 2 \cdot 2 + 1.$$

Substituting gives $1 = (-17)(7) + (3)(40)$, so an inverse is -17 . Since we are using this as an exponent, we need a non-negative inverse, so we can take $\bar{e} = -17 + 40 = 23$.

Answer:

23

6. (a) Evaluate $\left(\frac{101}{7}\right)$.

The quadratic residues of 7 are $1^2 = 1$, $2^2 = 4$, and $3^2 \equiv 2 \pmod{7}$. Since $101 \equiv 3 \pmod{7}$, 101 is not a quadratic residue of 7 so $\left(\frac{101}{7}\right) = -1$.

Answer:

-1

(b) Use the result of 6a to evaluate $\left(\frac{7}{101}\right)$.

By the Law of Quadratic Reciprocity, $\left(\frac{7}{101}\right) = \left(\frac{101}{7}\right) (-1)^{\frac{101-1}{2} \cdot \frac{7-1}{2}} = (-1)(-1)^{150} = -1$.

Answer:

-1