King Fahd University of Petroleum and Minerals

Department of Mathematics and Statistics

Math 455, Exam II, Term 142

Part I (20 points)

1. Decipher the message "ACMEMCBH" if it is enciphered using the affine cipher $C \equiv 3P + 2 \ mod \ 26$.
2. In an RSA cipher, on chooses the primes $p = 89$ and $q = 97$ and the enciphering exponent $e = 5$. Find the deciphering exponent.

Part II (40 points)

3. Show that $R_4 = 1111 = 11 \times 101$ is a pseudoprime to base 6.
4. Evaluate the sum $\sum_{d|n} \mu(d) \frac{\varphi(d)}{d}$, where n is a positive integer.
5. Solve the system

$$\begin{cases} x^3 - 2x + 1 \equiv 0 \ mod \ 5 \\ 3x \equiv 2 \ mod \ 4 \end{cases}$$

6. Find the smallest positive integer n such that $\tau(n) = 15$.

Part III (40 points)

7. Let $m > 1$ be an odd positive integer. Prove that the sum of the elements of any complete residue system modulo m is divisible by m. **(8 points)**

8. (a) Show that $\sigma(kn) > k\sigma(n)$ for any positive integers $k \geq 2$ and n. **(8 points)**

(b) Use part (a) to prove that if n is a perfect number or an abundant number, then kn is an abundant number for any positive integer $k \geq 2$. **(6 points)**

9. Prove that $\varphi(mn) = m\varphi(n)$ if every prime that divides m also divides n. **(8 points)**

10. Prove that some power of 27 ends with 00001. **(10 points)**

All the best,

Ibrahim Al-Rasasi

The Solutions

Question #1: We first solve for P in terms of C. Clearly the multiplicative inverse of 3 modulo 26 is 9. So multiplying the given congruence by 9, we get $P = 9C - 18\ mod 26$. The computation is performed in the following table.

Ciphertext	A	C	M	E	M	C	B	H
$C\#$	00	02	12	04	12	02	01	07
$P\#$	08	00	12	18	12	00	17	19
Plaintext	I	A	M	S	M	A	R	T

The original message is “IAMSMART” which is “I AM SMART”.

Question #2: Note first that $\varphi(n) = (p-1)(q-1) = 88 \times 96 = 8448$ and $\big(e, \varphi(n)\big) = 1$. The deciphering exponent d is the multiplicative inverse of e modulo $\varphi(n)$: $5d \equiv 1 mod\ 8448$. We solve this linear congruence:

$$5d \equiv 1 \equiv 8449 \equiv 16897 \equiv 25345\ mod\ 8448$$

This implies that $d \equiv 5069\ mod\ 8448$. Thus we may take $d = 5069$.

Question #3: We need to show that $6^{R_4 - 1} \equiv 1 mod\ R_4$. As $(R_4, 6) = (11 \times 101, 6) = 1$, then $(11,6) = 1$ and $(101,6) = 1$. By Fermat’s Theorem, we get

$$6^{10} \equiv 1 mod 11 \xrightarrow{111th\ power} 6^{R_4 - 1} \equiv 1 mod 11 \cdots (1)$$

$$6^{100} \equiv 1 mod 101 \xrightarrow{11th\ power} 6^{1100} \equiv 1 mod 101 \xrightarrow{\times 6^{10}} 6^{R_4 - 1} \equiv 6^{10} mod 101$$

But $6^{10} \equiv 6 \times 6^3 \times 6^3 \equiv 6 \times 14 \times 14 \equiv 6 \times 17 \equiv 102 \equiv 1 mod 101$. Then

$$6^{R_4 - 1} \equiv 1 mod 101 \cdots (2)$$

From (1) and (2), we conclude that $6^{R_4 - 1} \equiv 1 mod[11,101]$ and hence

$$6^{R_4 - 1} \equiv 1 mod\ R_4.$$

Question #4: Let $F(n)=\sum_{d|n}\mu(d)\frac{\varphi(d)}{d}$. Since $\mu,\varphi, and\ g(n)=n$ are multiplicative functions, then so is $\frac{\mu\varphi}{g}$ and hence so is F. Thus we start evaluating F at a prime power p^α:

$$F(p^\alpha)=\sum_{d|p^\alpha}\mu(d)\frac{\varphi(d)}{d}=\sum_{i=0}^{\alpha}\mu(p^i)\frac{\varphi(p^i)}{p^i}$$

$$=\mu(1)\frac{\varphi(1)}{1}+\mu(p)\frac{\varphi(p)}{p}+0=1-\frac{p-1}{p}=\frac{1}{p}$$

Now if $n=\prod_{i=1}^{r}p_i^{\alpha_i}$, then

$$F(n)=\prod\nolimits_{i=1}^{r}F(p_i^{\alpha_i})=\prod\nolimits_{i=1}^{r}\frac{1}{p_i}=\left(\prod_{p|n}p\right)^{-1}.$$

Question #5: The first congruence has the two solutions $x\equiv 1,2\ mod 5$ and the second congruence has one solution $x\equiv 2\ mod 4$. We construct the following two systems:

$$(1)\begin{cases}x\equiv 1\ mod 5\\ x\equiv 2\ mod 4\end{cases}\qquad(2)\begin{cases}x\equiv 2\ mod 5\\ x\equiv 2\ mod 4\end{cases}$$

Using the Chinese Remainder Theorem, we get the solutions $x\equiv 2,6\ mod 20$.

Question #6: Since $15=3\times 5$, then all possible solutions of $\tau(n)=15$ are $p^{14}\ and\ p^2q^4$, where $p\ and\ q$ are primes. The smallest solution of the form p^{14} is $2^{14}=16384$, and the smallest solution of the form p^2q^4 is $3^2\times 2^4=144$. Thus the smallest solution of the equation $\tau(n)=15$ is $n=144$.

Question #7: Let $m>1$ be an odd positive integer and let $S=\{c_1,c_2,\cdots,c_m\}$ be a complete residue system modulo m. The set $T=\{0,1,\cdots,m-1\}$ is also a complete residue system modulo m. This implies that each element of S is congruent to an element of T (since T is a complete residue system modulo m) and no two elements of S are congruent to the same element of T (since S is a complete residue system modulo m.) This implies that

$$c_1+c_2+\cdots+c_m\equiv 0+1+\cdots+(m-1)\ mod\ m$$

$$\equiv \frac{m-1}{2} \times m$$

$$\equiv 0 \; mod \; m$$

(Note that $\frac{m-1}{2}$ is an integer since m is odd.) We conclude that the sum of the elements of any complete residue system modulo m is divisible my m.

Question #8: (a) Let $d_1, d_2, \cdots, d_r$, where $d_1 = 1, d_r = n, and\; r = \tau(n)$, be the positive divisors of n. Then $kd_1, kd_2, \cdots, kd_r$, are divisors of kn, but not all of the divisors of kn (as, for example, 1 is not included in the list $kd_1, kd_2, \cdots, kd_r$). This implies that

$$\sigma(kn) > kd_1 + kd_2 + \cdots + kd_n = k\sigma(n).$$

Now for part (b), the assumption implies that $\sigma(n) \geq 2n$. This implies that

$$\sigma(kn) > k\sigma(n) \geq k(2n)$$

or

$$\sigma(kn) > 2kn$$

and hence kn is an abundant number.

Question #9: Use the formula for φ:

$$\varphi(mn) = mn \prod_{p|mn} \left(1 - \frac{1}{p}\right) = mn \prod_{p|n} \left(1 - \frac{1}{p}\right) = m\varphi(n),$$

where the second equality follows from the assumption of the question.

Question #10: Read in a different way, the question says that the last five digits (from the right) of some power of 27 is 00001. So we can take the power to be $\varphi(10^5)$ as by Euler's Theorem, we have

$$27^{\varphi(10^5)} \equiv 1 \equiv 00001 \; mod \; 10^5.$$