King Fahd University of Petroleum & Minerals

Department of Mathematics & Statistics

Math 427, Exam II, Term 181

Part I (70 points)

1. **[8 points]** Show that $n = 2465 = 5 \cdot 17 \cdot 29$ is a Carmichael number.
2. **[10 points]** Solve $\phi(n) = 8$ in positive integers.
3. **[10 points]** Find the smallest three positive and consecutive integers greater than 10 that are divisible respectively by 9, 10, and 11.
4. **[10 points]** Solve the polynomial congruence

$$x^3 + 3x + 1 \equiv 0 \; mod \; 5^3.$$

5. **[10 points]** Decide if Mersenne number $M_{23} = 2^{23} - 1$ is prime or composite.
6. **[14 points]**
   a. Show that 2 is a primitive root modulo 13.
   b. Find a reduced residue system modulo 13 consisting entirely of powers of some integer.
   c. Find all primitive roots modulo 13.
   d. Solve the congruence $9 \cdot 7^x \equiv 5 \; mod \; 13$ in positive integers.
7. **[8 points]** Decipher the message "QJVROU" if it is enciphered using the affine cipher $C \equiv 15P + 1 \; mod \; 26$.

Part II (30 points)

8. **[10 points]** Prove that if g is a primitive root modulo $m > 1$, then $\bar{g}$ is also a primitive root modulo m. [$\bar{g}$ is the multiplicative inverse of g modulo m.]
9. **[10 points]** Let $p > 2$ be a prime. Prove that -1 is a 6th power residue modulo p if and only if $p \equiv 1, 5 \; mod \; 12$.

10. [10 points] Prove that if $n+2$ is prime, then

$$4[(n-1)!+1]+n \equiv 0 \; mod \; (n+2).$$

All the best,

Ibrahim Al-Rasasi

A	B	C	D	E	F	G	H	I	J	K	L	M
00	01	02	03	04	05	06	07	08	09	10	11	12

N	O	P	Q	R	S	T	U	V	W	X	Y	Z
13	14	15	16	17	18	19	20	21	22	23	24	25

Solutions

Q1: Let a be an integer such that $(a,n)=1$. To show that $n=2465=5\cdot17\cdot29$ is a Carmichael number, we need to show that $a^{n-1}\equiv 1\ mod\ n$.

Since $(a,n)=1$, then $(a,5)=(a,17)=(a,29)=1$. By using Fermat's theorem and noticing that

$$n-1=2464=4\cdot616=16\cdot154=28\cdot88,$$

we get

$$a^4\equiv 1\ mod\ 5 \xRightarrow{616th\ power} a^{n-1}\equiv 1\ mod\ 5$$

$$a^{16}\equiv 1\ mod\ 17 \xRightarrow{154th\ power} a^{n-1}\equiv 1\ mod\ 17$$

$$a^{28}\equiv 1\ mod\ 29 \xRightarrow{88th\ power} a^{n-1}\equiv 1\ mod\ 29$$

This implies $a^{n-1}\equiv 1\ mod[5,17,29], or\ a^{n-1}\equiv 1\ mod\ n$, and hence $n=2465$ is a Carmichael number.

Q2: We start by investigating the possible properties of the solutions of the equation $\phi(n)=8$.

Let p be a prime and n be a possible solution. If $p|n$, then $\phi(p)|\phi(n)$ and hence $p-1|8$. This implies that $p\in\{2,3,5\}$. Further,

$$2^\alpha|n \overset{\phi}{\Rightarrow} 2^{\alpha-1}|8 \Rightarrow \alpha\le 4,$$

$$3^\beta\,\Big|n \overset{\phi}{\Rightarrow} 3^{\beta-1}\cdot 2\Big|\,8 \Rightarrow \beta=1,$$

$$5^\gamma\,\Big|n \overset{\phi}{\Rightarrow} 5^{\gamma-1}\cdot 4\Big|\,8 \Rightarrow \gamma=1.$$

Thus, a possible solution has the form

$$n = 2^{\alpha} \cdot 3^{\beta} \cdot 5^{\gamma}, \qquad 0 \le \alpha \le 4, 0 \le \beta \le 1, 0 \le \gamma \le 1.$$

This gives $5 \times 2 \times 2 = 20$ candidates for possible solutions:

$$n = 1,3,5, \boxed{3 \cdot 5}, 2, 2 \cdot 3, 2 \cdot 5, \boxed{2 \cdot 3 \cdot 5}, 2^2, 2^2 \cdot 3, \boxed{2^2 \cdot 5}, 2^2 \cdot 3 \cdot 5,$$

$$2^3, \boxed{2^3 \cdot 3}, 2^3 \cdot 5, 2^3 \cdot 3 \cdot 5, \boxed{2^4}, 2^4 \cdot 3, 2^4 \cdot 5, 2^4 \cdot 3 \cdot 5.$$

The solutions are the numbers in the boxes:

$$n = 15, 16, 20, 24, 30.$$

Q3: The problem reduces to solving the linear system

$$\begin{cases} x \equiv 0 \; mod \; 9 \\ x + 1 \equiv 0 \; mod \; 10 \\ x + 2 \equiv 0 \; mod \; 11 \end{cases}$$

Solving, we get the unique solution $x \equiv 9 \; mod \; 990$. Thus all integer solutions of the system are given by $x = 9 + 990k$, where k is an integer. The smallest positive solution greater than 10 is $x = 999$ (when $k = 1$). The three required integers are $999, 1000, 1001$.

Q4: Let $f(x) = x^3 + 3x + 1$. Then $f'(x) = 3x^2 + 3$. The congruence $f(x) \equiv 0 mod \; 5$ has two solutions $a_1 \equiv 1 \; mod \; 5 \; and \; b_1 \equiv 2 \; mod \; 5$.

Now $f'(b_1) \equiv 15 \equiv 0 \; mod \; 5$. Then b_1 is a singular solution. Since $f(b_1) \equiv 15 \neq 0 \; mod \; 5^2$, then b_1 cannot be lifted to a solution for the congruence $f(x) \equiv 0 \; mod \; 5^2$, and hence it cannot be lifted to a solution for the congruence $f(x) \equiv 0 \; mod \; 5^3$.

Next, $f'(a_1) \equiv 6 \neq 0 \; mod \; 5$. Then a_1 is a nonsingular solution and hence it can be lifted indefinitely. With $a_1 = 1$,

$$a_2 \equiv a_1 - f(a_1)\overline{f'(a_1)} \; mod \; 5^2$$
$$\equiv 1 - 5 \cdot 1 \equiv -4 \; mod \; 5^2$$

With $a_2 = -4$,

$$a_3 \equiv a_2 - f(a_2)\overline{f'(a_2)} \; mod \; 5^3$$
$$\equiv -4 - (-75) \cdot 1 \equiv 71 \; mod \; 5^3.$$

Thus, there is one solution $x \equiv 71 \; mod \; 5^3$ for the congruence $x^3 + 3x + 1 \equiv 0 \; mod \; 5^3$.

Q5: Note first that $M_{23} = 2^{23} - 1 = 8388607$. If q is a prime such that $q|M_{23}$, then $q = 2k \cdot 23 + 1 = 46k + 1$ for some positive integer k. Further, if M_{23} is composite, then it has a prime divisor less than or equal to $\sqrt{M_{23}} \approx 2896.3$. So we check the values of k such that $46k + 1 \leq 2896$. These values are $k \leq 62$. If $k = 1$, then $q = 47$ and we find that $47|M_{23}$. In fact, $M_{23} = 47 \cdot 178481$. So, M_{23} is composite.

Q6:

Part a: Compute the powers of 2 modulo 13(to be used also later):

$$2^1 \equiv 2, 2^2 \equiv 4, 2^3 \equiv 8, 2^4 \equiv 3, 2^5 \equiv 6, 2^6 \equiv 12,$$
$$2^7 \equiv 11, 2^8 \equiv 9, 2^9 \equiv 5, 2^{10} \equiv 10, 2^{11} \equiv 7, 2^{12} \equiv 1$$

Since the order of 2 modulo 13 is $12 = \phi(13)$, then 2 is a primitive root modulo 13.

Part b: The set $\{2, 2^2, 2^3, \cdots, 2^{12}\}$ is a reduced residue system modulo 13 consisting entirely of powers of 2 (as can be readily observed from the calculation in part (a)).

Part c: In terms of the primitive root 2, all primitive roots modulo 13 are given by

$$\{2^i : (i,12) = 1\} = \{2^i : i = 1,5,7,11\} = \{2, 2^5, 2^7, 2^{11}\}.$$

Modulo 13, they are $2, 6, 7, 11$.

Part d: From part (a), note that $5 \equiv 2^9, 7 \equiv 2^{11}, 9 \equiv 2^8 \ mod\ 13$. Thus the congruence $9 \cdot 7^x \equiv 5\ mod\ 13$ becomes $2^{8+11x} \equiv 2^9\ mod\ 13$ which reduces to the linear congruence $8 + 11x \equiv 9\ mod\ 12$. This linear congruence has a unique solution $x \equiv 11\ mod\ 12$, which is the solution of the given congruence (we take the positive solutions: $x = 11 + 12k, k \geq 0$.)

Q7: To decipher, we solve for P in terms of C. The inverse of 15 modulo 26 is 7. So we get $P \equiv 7(C-1) mod\ 26$.

	Q	J	V	R	O	U
C	16	09	21	17	14	20
P	01	04	10	08	13	03
	B	E	K	I	N	D

The original message is “BE KIND”.

Q8: Since g is a primitive root modulo m, then $ord_m(g) = \phi(m)$ and also $g^{\phi(m)} \equiv 1\ mod\ m$. Let $ord_m(\bar{g}) = h$. Then $h|\phi(m)$ and hence $1 \leq h \leq \phi(m)$. We will show that $h = \phi(m)$.

Assume that $h < \phi(m)$. Since $g\bar{g} \equiv 1 mod\ m$, then raising both sides to power h, we get $g^h \bar{g}^h \equiv 1\ mod\ m$ and hence $g^h \equiv 1\ mod\ m$; a contradiction to the minimality of $\phi(m)$ ($h < \phi(m)$ and $\phi(m)$ is the smallest positive integer such that $g^{\phi(m)} \equiv 1\ mod\ m$.) Thus $h = \phi(m)$ and so $\bar{g}$ is a primitive root modulo m.

Q9: The integer -1 is a 6th power residue modulo $p > 2$ (i.e., $x^6 \equiv -1 \; mod \; p$ is solvable) if and only if

$$(-1)^{\frac{p-1}{(6,p-1)}} \equiv 1 \; mod \; p \; \cdots\cdots (*)$$

Clearly, $(*)$ does not hold when $p = 3 \; (as \; (-1)^1 \neq 1 \; mod \; 3.)$ Now, any prime $p > 3$ takes one of the following forms

$$p \equiv 1, 5, 7, or \; 11 \; mod \; 12.$$

We check each form separately.

If $p \equiv 1 \; mod \; 12$, then $p = 1 + 12k$ where $k > 0$ is an integer. As $(6, p-1) = 6$, then

$$(-1)^{\frac{p-1}{(6,p-1)}} \equiv (-1)^{2k} \equiv 1 \; mod \; p.$$

If $p \equiv 5 \; mod \; 12$, then $p = 5 + 12k$ where $k \geq 0$ is an integer. As $(6, p-1) = 2$, then

$$(-1)^{\frac{p-1}{(6,p-1)}} \equiv (-1)^{2+6k} \equiv 1 \; mod \; p.$$

If $p \equiv 7 \; mod \; 12$, then $p = 7 + 12k$ where $k \geq 0$ is an integer. As $(6, p-1) = 6$, then

$$(-1)^{\frac{p-1}{(6,p-1)}} \equiv (-1)^{1+2k} \equiv -1 \; mod \; p.$$

If $p \equiv 11 \; mod \; 12$, then $p = 11 + 12k$ where $k \geq 0$ is an integer. As $(6, p-1) = 2$, then

$$(-1)^{\frac{p-1}{(6,p-1)}} \equiv (-1)^{5+6k} \equiv -1 \; mod \; p.$$

From the above discussion, we conclude that $(*)$ holds (i.e., -1 is a 6th power residue modulo p) if and only if $p \equiv 1, 5 \; mod \; 12$.

Q10: Since $n + 2$ is prime, then, by Wilson's Theorem,

$$(n + 1)! \equiv -1 \equiv n + 1 \ mod \ (n + 2).$$

As $(n + 1, n + 2) = 1$, then

$$n! \equiv 1 \ mod \ (n + 2).$$

Note that $n! \equiv n \cdot (n - 1)! \equiv -2 \cdot (n - 1)! \ mod \ (n + 2)$. Then we get

$$-2 \cdot (n - 1)! \equiv 1 \ mod \ (n + 2).$$

Multiplying by -2, we get

$$4 \cdot (n - 1)! \equiv -2 \equiv n \ mod \ (n + 2).$$

Adding $4 + n$, we obtain

$$4 \cdot (n - 1)! + 4 + n \equiv 2n + 4 \equiv 2(n + 2) \ mod \ (n + 2),$$

or,

$$4[(n - 1)! + 1] + n \equiv 0 \ mod \ (n + 2).$$