KFUPM

Department of Mathematics

Math 427, Exam II, Term 242.

Part I (60 points)

1. **[15 points]** Solve $\phi(n) = 8$ in positive integers.
2. **[10 points]** Solve $2x^{123} - x^{80} + 2 \equiv 0 \; mod \; 7$.
3. **[10 points]** Solve $x^3 - 2x^2 + x - 2 \equiv 0 \; mod \; 7^2$.
4. **[15 points]**
   a. Decipher "QJO" if it is enciphered by the affine cipher $C \equiv 3P + 1 \; mod \; 26$.
   b. In an RSA cipher, $n = 1483483 \; and \; \phi(n) = 1481040$. Find the prime factors of n.
5. **[10 points]** Find the number of zeros at the right end of $\frac{(1111)!}{(111)!^{10}}$.

Part II (40 points)

6. **[10 points]** Prove that $\phi(n^3) = n^2\phi(n)$ for any integer $n \geq 1$.
7. **[10 points]** Describe all integers a for which the following congruence has three solutions: $(a + 4)x^2 + (a^3 - 2) \equiv 0 \; mod \; 3$.
8. **[10 points]** Let $p > 2$ be a prime number and $d > 0$ be an integer such that $d|p - 1$. Prove that the congruence $x^d \equiv 1 \; mod \; p^k$ has d solutions for each integer $k \geq 1$. **Hint:** Use Hensel's Lemma.
9. **[10 points]** Let x be a real number. Prove that $5[\![2x]\!] \leq [\![4x]\!] + [\![6x]\!]$.

Good luck,

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: Solve $\phi(n) = 8$ in positive integers.

Solution: We start by ruling out some possibilities of an integer n to be a solution.

If n is divisibly by three distinct odd primes $p, q\ and\ r$, then

$$pqr \Big| n \Rightarrow \phi(pqr) \Big| \phi(n) \Rightarrow (p-1)(q-1)(r-1)|8,$$

which is not possible since $(p-1)(q-1)(r-1) \geq (3-1)(5-1)(7-1) > 8$. So, n can have at most two distinct odd primes.

If $2^\alpha|n, \alpha \geq 5$, then

$$\phi(2^\alpha)|\phi(n) \Rightarrow 2^{\alpha-1}|8$$

which is not possible since $16|2^{\alpha-1}$.

If $p^\alpha|n,\ (p\ is\ an\ odd\ prime, \alpha \geq 2)$, then

$$\phi(p^\alpha)|\phi(n) \Rightarrow p^{\alpha-1}(p-1)|8 \Rightarrow p|8,$$

which is not possible for an odd prime p.

The above analysis implies that a solution of the equation $\phi(n) = 8$ has to have one of the following forms:

$$n = 2^\alpha, p, 2^\alpha p, pq, 2^\alpha pq,$$

where $p\ and\ q$ are distinct odd primes (say $p < q$) and $1 \leq \alpha \leq 4$.

Now

- $n = 2^\alpha \overset{\phi}{\Rightarrow} 8 = 2^{\alpha-1} \Rightarrow \alpha = 4 \Rightarrow n = 16,$
- $n = p \overset{\phi}{\Rightarrow} 8 = p - 1 \Rightarrow p = 9$, not prime,
- $n = 2^\alpha p \overset{\phi}{\Rightarrow} 8 = 2^{\alpha-1}(p-1) \Rightarrow (\alpha, p) = (2,5), (3,3) \Rightarrow n = 20, 24,$
- $n = pq \overset{\phi}{\Rightarrow} 8 = (p-1)(q-1) \Rightarrow p = 3, q = 5 \Rightarrow n = 15,$
- $n = 2^\alpha pq \overset{\phi}{\Rightarrow} 8 = 2^{\alpha-1}(p-1)(q-1) \Rightarrow (\alpha, p, q) = (1,3,5) \Rightarrow n = 30.$

We conclude that the solutions of the equation $\phi(n) = 8$ are $n = 15, 16, 20, 24, 30$.

Q2: Solve $2x^{123} - x^{80} + 2 \equiv 0 \ mod\ 7$.

Solution: First we reduce the power of the polynomial congruence. By Fermat's Theorem, $a^7 \equiv a \ mod\ 7$ for any integer a. This implies

$$a^{80} = a^{77}a^3 \equiv a^{11}a^3 = a^{14} \equiv a^2 \ mod\ 7,$$

$$a^{123} = a^{17\times 7}a^4 \equiv a^{17}a^4 = a^{21} \equiv a^3 \ mod\ 7.$$

Thus, the given congruence is equivalent to the congruence

$$2x^3 - x^2 + 2 \equiv 0 \ mod\ 7.$$

By checking $CRS_7 = \{0, \pm 1, \pm 2, \pm 3\}$, we find that the congruence has one solution $x \equiv 2 \ mod\ 7$.

Q3: Solve $x^3 - 2x^2 + x - 2 \equiv 0 \ mod\ 7^2$.

Solution: Checking $CRS_7 = \{0, \pm 1, \pm 2, \pm 3\}$, we see that the congruence

$$x^3 - 2x^2 + x - 2 \equiv 0 \ mod\ 7$$

has one solution $x_1 \equiv 2 \ mod\ 7$ only.

Let $f(x) = x^3 - 2x^2 + x - 2$. Then $f'(x) = 3x^2 - 4x + 1$. Since $f'(2) = 5 \not\equiv 0 \ mod\ 7$, then x_1 is a nonsingular solution for $f(x) \equiv 0 \ mod\ 7$, hence it can be lifted to a unique solution for $f(x) \equiv 0 \ mod\ 7^2$ and the solution is given by

$$x_2 \equiv x_1 - f(x_1)\,\overline{f'(x_1)} \ mod\ 7^2$$

$$\equiv 2 - 0 \cdot \overline{5} \ mod\ 7^2.$$

Thus $x_2 \equiv 2 \ mod\ 7^2$ is the solution of $f(x) \equiv 0 \ mod\ 7^2$.

Q4:

Part (a): Decipher "QJO" if it is enciphered by the affine cipher $C \equiv 3P + 1 \; mod \; 26$.

Solution: Multiplying by 9, we get $9C \equiv P + 9 \; mod \; 26$ and hence

$$P \equiv 9(C - 1) \; mod \; 26.$$

$$Q \leftrightarrow 16: P \equiv 9(15) \equiv 5 \; mod \; 26; 5 \leftrightarrow F,$$

$$J \leftrightarrow 9: P \equiv 9(8) \equiv 20 \; mod \; 26; 20 \leftrightarrow U,$$

$$O \leftrightarrow 14: P \equiv 9(13) \equiv 13 \; mod \; 26; 13 \leftrightarrow N.$$

The original message is "FUN".

Part (b): In an RSA cipher, $n = 1483483 \; and \; \phi(n) = 1481040$. Find the prime factors of n.

Solution: As $n = 1483483 \; and \; \phi(n) = 1481040$, then

$$p + q = n - \phi(n) + 1 = 2444,$$

$$p - q = \sqrt{(p+q)^2 - 4n} = \sqrt{39204} = 198.$$

Adding, we get $2p = 2642$ and hence $p = 1321$. Using the first equation, we get $q = 1123$.

Q5: Find the number of zeros at the right end of $\frac{(1111)!}{(111)!^{10}}$.

Solution: Let $5^{\alpha} || (1111)!$ And $5^{\beta} || (111)!$. Note first that $1111 < 5^5$ and $111 < 5^3$. Then we have

$$\alpha = \sum_{i=1}^{\infty} \left[\left[\frac{1111}{5^i}\right]\right] = \left[\left[\frac{1111}{5}\right]\right] + \left[\left[\frac{1111}{25}\right]\right] + \left[\left[\frac{1111}{125}\right]\right] + \left[\left[\frac{1111}{625}\right]\right]$$

$$= 222 + 44 + 8 + 1 = 275.$$

$$\beta = \sum_{i=1}^{\infty} \left[\left[\frac{111}{5^i}\right]\right] = \left[\left[\frac{111}{5}\right]\right] + \left[\left[\frac{111}{25}\right]\right] = 22 + 4 = 26.$$

The number of zeros at the right end of $\frac{(1111)!}{(111)!^{10}}$ is $275 - 26(10) = 15$.

Q6: Prove that $\phi(n^3) = n^2\phi(n)$ for any integer $n \geq 1$.

Solution: We use the formula of ϕ:

$$\phi(n^3) = n^3 \prod\nolimits_{p|n^3} \left(1 - \frac{1}{p}\right)$$

$$= n^3 \prod\nolimits_{p|n} \left(1 - \frac{1}{p}\right)$$

$$= n^2 \left[n \prod\nolimits_{p|n} \left(1 - \frac{1}{p}\right)\right] = n^2\, \phi(n).$$

The second equality follows because $p|n^3$ if and only if $p|n$.

Q7: Describe all integers a for which the following congruence has three solutions: $(a+4)x^2 + (a^3 - 2) \equiv 0 \; mod\; 3$.

Solution: By Lagrange's Theorem, if the degree of the polynomial congruence $f(x) \equiv 0 \; mod\; p, (p\; is\; prime)$, is n, then it has at most n solutions. In our case, for the number of solutions (3) to be more than the degree (2), then the polynomial congruence must be the zero congruence: that is,

$$a + 4 \equiv 0 \; mod\; 3 \; and\; a^3 - 2 \equiv 0 \; mod\; 3.$$

Solve each congruence:

$$a + 4 \equiv 0 \; mod\; 3 \Rightarrow a \equiv 2 \; mod\; 3,$$

$$a^3 - 2 \equiv 0 \; mod\; 3 \Rightarrow a \equiv 2 \; mod\; 3.$$

We conclude that the given congruence has three solutions if and only if $a \equiv 2 \; mod\; 3$.

Q8: Let $p > 2$ be a prime number and $d > 0$ be an integer such that $d|p-1$. Prove that the congruence $x^d \equiv 1 \; mod \; p^k$ has d solutions for each integer $k \geq 1$.

Solution: The case $k = 1$ is a lemma in the course; that is, since $d|p-1$, then the congruence

$$x^d \equiv 1 \; mod \; p \cdots\cdots (*)$$

has d solutions.

Let $k \geq 2$ be an integer. Let $f(x) = x^d - 1$. Then $f'(x) = d\, x^{d-1}$.

Let x_0 be one solution of $(*)$: $f(x_0) \equiv 0 \; mod \; p$ (which is the same thing as $x_0^d \equiv 1 \; mod \; p$). Since $d|p-1$, then $d \leq p-1 < p$ and hence $(d,p) = 1$. Also, as $x_0^d \equiv 1 \; mod \; p$, then $\left(x_0^d, p\right) = (1,p) = 1$ and hence $(x_0, p) = 1$. We conclude that $f'(x_0) = d\, x_0^{d-1} \not\equiv 0 \; mod \; p$, and hence x_0 is a nonsingular solution. By Hensel's Lemma, x_0 can be lifted to a unique solution for the congruence $f(x) \equiv 0 \; mod \; p^k$ for every integer $k \geq 2$. Since $(*)$ has d nonsingular solutions, and each one can be lifted to a unique solution for $f(x) \equiv 0 \; mod \; p^k$ (for each integer $k \geq 2$), then the congruence $f(x) \equiv 0 \; mod \; p^k$ has d solutions for each integer $k \geq 1$.

Q9: Let x be a real number. Prove that $5[\![2x]\!] \leq [\![4x]\!] + [\![6x]\!]$.

Solution: We use the inequality

$$[\![z]\!] + [\![w]\!] \leq [\![z+w]\!], \qquad z, w \in \mathbb{R}.$$

We proceed as follows:

$$\begin{aligned} 5[\![2x]\!] &= [\![2x]\!] + ([\![2x]\!] + [\![2x]\!]) + ([\![2x]\!] + [\![2x]\!]) \\ &\leq [\![2x]\!] + [\![4x]\!] + [\![4x]\!] \\ &\leq [\![4x]\!] + [\![2x + 4x]\!]. \end{aligned}$$

Thus, $5[\![2x]\!] \leq [\![4x]\!] + [\![6x]\!]$.