King Fahd University of Petroleum & Minerals

Department of Mathematics & Statistics

Math 427, Final Exam, Term 181

Saturday, Dec. 15, 2018

Part I (100 points)

1. **[8 points]** Find all positive integers $x \; and \; y$ such that $(x, y) = 6$ and $[x, y] = 72$. You may assume that $x > y$.
2. **[10 points]** Find the last three digits from the right of the number 6^{1000}.
3. **[8 points]** Solve the polynomial congruence $x^5 + x + 1 \equiv 0 \; mod \; 35$.
4. **[8 points]** In an RSA cipher, $n = 18556567 \; and \; \phi(n) = 18547936$. Find the prime factors of n.
5. **[6 points]** Find the quadratic residues modulo 13.
6. **[10 points]** Find all integers $n \geq 1$ that satisfy the equation $[\![\sqrt{n}]\!] = [\![\sqrt{n+1}]\!]$.
7. **[14 points]** Find all primes $p > 5$ for which the congruence $x^2 + 45 \equiv 0 \; mod \; p$ is solvable.
8. **[14 points]** Find all primitive Pythagorean triples (x, y, z), with y even, in which x is a perfect cube.
9. **[12 points]**
   a. Find the sum $\sum_{d|n} \frac{\mu(d)}{d^2}$.
   b. Let f be an arithmetic function. If $\sum_{d|n} df(d) = n^2$, then find f.
10. **[10 points]** Find the integer solutions of $x^2 - y^2 = 6y + 6$.

Part II (75 points)

11. **[15 points]** Prove that $396|n^{30}-1$ for all integers n such that $(n,396)=1$.

12. **[12 points]** Let $p>2$ be a prime number. Prove that a is a quadratic residue modulo p if and only if $\overline{a}$ is a quadratic residue modulo p. ($\overline{a}$ is the multiplicative inverse of a modulo p.)

13. **[13 points]** Prove that $\frac{(n!)!}{(n!)^{(n-1)!}}$ is an integer.

14. **[20 points]**

a. Prove that $2p^k$ is a deficient number for any prime $p \geq 5$ and any integer $k \geq 1$.

b. Classify the numbers $2 \cdot 3^k, k \geq 1$, as perfect, deficient, or abundant.

15. **[15 points]** Let n be a positive integer such that $p=8n+3 \; and \; q=4n+1$ are both primes. Prove that 2 is a primitive root modulo p.

All the best,

Ibrahim Al-Rasasi

<u>**Solutions**</u>

Q# 1: As $(x, y) = 6$, then $x = 6x_1\ and\ y = 6y_1$, where $(x_1, y_1) = 1$. Note also that under the assumption $x > y$, we have $x_1 > y_1$. Now,

$$[x, y] = 72 \Rightarrow 6[x_1, y_1] = 72 \Rightarrow x_1 y_1 = 12.$$

Since $x_1 > y_1\ and\ (x_1, y_1) = 1$, then this implies that $(x_1, y_1) = (12,1)$, $(4,3)$ and hence the solutions are

$$(x, y) = (72,6), (24,18).$$

Q# 2: Let $x = 6^{1000}$. Note that $1000 = 8 \cdot 125$. Clearly $x \equiv 0\ mod\ 8$. By Euler's theorem, $6^{\phi(125)} \equiv 1\ mod\ 125; i.e., 6^{100} \equiv 1\ mod\ 125$ and hence $6^{1000} \equiv 1\ mod\ 125, or\ x \equiv 1\ mod\ 125$. Next we solve the system:

$$\begin{cases} x \equiv 0\ mod\ 8 \\ x \equiv 1\ mod\ 125 \end{cases}$$

The first congruence gives $x = 8k$. The second congruence gives

$$8k \equiv 1 \equiv 126\ mod\ 125 \Rightarrow 4k \equiv 63 \equiv 188\ mod\ 125 \Rightarrow k \equiv 47\ mod\ 125.$$

Thus, $x = 8(47 + 125l) = 376 + 1000l, or\ x \equiv 376\ mod\ 1000$. So the number 6^{1000} ends with 376 (at the right).

Q# 3: The congruence $x^5 + x + 1 \equiv 0\ mod\ 35$ is equivalent to the system

$$\begin{cases} x^5 + x + 1 \equiv 0\ mod\ 5 \\ x^5 + x + 1 \equiv 0\ mod\ 7 \end{cases}$$

The first congruence has one solution $x \equiv 2 \, mod \, 5$ and the second congruence has two solutions $x \equiv 2, -3 \, mod \, 7$. This leads to the linear systems

$$\begin{cases} x \equiv 2 \, mod \, 5 \\ x \equiv 2 \, mod \, 7 \end{cases} \qquad \begin{cases} x \equiv 2 \equiv -3 \, mod \, 5 \\ x \equiv -3 \, mod \, 7 \end{cases}$$

The solutions of these linear systems are $x \equiv 2 \, mod \, 35, x \equiv -3 \, mod \, 35$ respectively. Thus, the solutions of the congruence $x^5 + x + 1 \equiv 0 \, mod \, 35$ are $x \equiv -3, 2 \, mod \, 35$.

Q# 4: $n = pq, \; n = 18556567, \; \phi(n) = 18547936$. We have

$$p + q = n - \phi(n) + 1 = 8632$$

$$p - q = \sqrt{(p+q)^2 - 4n} = \sqrt{285156} = 534$$

Adding, we get $2p = 9166$ and hence $p = 4583$. Substituting in either equation, we get $q = 4049$. So $n = 4049 \times 4583$.

Q# 5: The quadratic residues modulo 13 are

$$\{1^2, 2^2, 3^2, 4^2, 5^2, 6^2\} =_{mod\ 13} \{1,3,4,9,10,12\} =_{mod\ 13} \{\pm 1, \pm 3, \pm 4\}.$$

Q# 6: Let $k \geq 1$ be an integer and let $[\![\sqrt{n}]\!] = k$. Then $k \leq \sqrt{n} < k + 1$ and hence

$$k^2 \leq n < (k+1)^2.$$

This implies that (Where does $n + 1$ lie?)

$$k^2 \leq n < n + 1 \leq (k+1)^2.$$

Now we consider two cases:

Case I: $n+1$ is a square. In this case we must have $n+1=(k+1)^2$ and hence

$$[\![\sqrt{n+1}]\!] = k+1 \neq k = [\![\sqrt{n}]\!].$$

Case II: $n+1$ is not a square. In this case, we have

$$k^2 \leq n < n+1 < (k+1)^2.$$

This implies that

$$k \leq \sqrt{n} < \sqrt{n+1} < k+1$$

and hence $[\![\sqrt{n}]\!] = [\![\sqrt{n+1}]\!]$.

We conclude that $[\![\sqrt{n}]\!] = [\![\sqrt{n+1}]\!]$ when $n \neq m^2-1$, where m is a positive integer.

Q# 7: Let $p>5$ be a prime. Note that $(p,-45)=1$. The congruence $x^2+45 \equiv 0 \; mod \; p$ is solvable if and only if $\left(\frac{-45}{p}\right)=1$. As $-45=-1 \cdot 3^2 \cdot 5$, then

$$\left(\frac{-45}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{3^2}{p}\right)\left(\frac{5}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{5}{p}\right) \cdots\cdots (*)$$

Now

$$\left(\frac{-1}{p}\right) = \begin{cases} 1 \;\; if \; p \equiv 1 mod 4 \\ -1 \;\; if \; p \equiv 3 mod 4. \end{cases}$$

Next, we compute $\left(\frac{5}{p}\right)$. We use the quadratic reciprocity law and the properties of Legendre symbol:

$$\left(\frac{5}{p}\right) =_{QRL} \left(\frac{p}{5}\right) = \begin{cases} 1 \;\; if \; p \equiv 1,4 mod 5 \\ -1 \; if \; p \equiv 2,3 mod 5. \end{cases}$$

Now, $(*)$ implies that $\left(\frac{-45}{p}\right) = 1$ if and only if

$$\left(\frac{-1}{p}\right) = \left(\frac{5}{p}\right) = 1\,; \left(\frac{-1}{p}\right) = \left(\frac{5}{p}\right) = -1.$$

The first case holds when

$$\begin{cases} p \equiv 1 mod 4 \\ p \equiv 1 mod 5 \end{cases}, \qquad \begin{cases} p \equiv 1 mod 4 \\ p \equiv 4 mod 5 \end{cases}$$

This leads to $p \equiv 1,9 \; mod \; 20$. The second case holds when

$$\begin{cases} p \equiv -1 mod 4 \\ p \equiv 2 mod 5 \end{cases}, \qquad \begin{cases} p \equiv -1 \equiv 3 mod 4 \\ p \equiv 3 mod 5 \end{cases}$$

This leads to $p \equiv 7,3 \; mod \; 20$.

Thus, if $p > 5$, the given congruence is solvable if and only if $p \equiv 1,3,7,9 \; mod \; 20$.

Q# 8: If (x, y, z) is primitive Pythagorean triple, with y even, then

$$x = r^2 - s^2, y = 2rs, z = r^2 + s^2$$

where $r \; and \; s$ are positive integers of opposite parity, $r > s$, and $(r, s) = 1$. If x is a perfect cube, then there is a positive integer u such that $x = u^3, or, r^2 - s^2 = u^3$. This implies that

$$u^3 = (r - s)(r + s).$$

Since $(r - s, r + s) = 1$ (left for you to check), then there are positive integers $m \; and \; n$ such that

$$r - s = m^3, \qquad r + s = n^3.$$

This implies that $m \; and \; n$ are odd, $n > m$, and $(m, n) = 1$. Solving, we get

$$r = \frac{n^3+m^3}{2}, \; s = \frac{n^3-m^3}{2}.$$

Thus, the required triples are (x, y, z), where

$$x = r^2 - s^2 = (mn)^3, y = 2rs = \frac{n^6 - m^6}{2}, z = r^2 + s^2 = \frac{n^6 + m^6}{2}$$

where $m \; and \; n$ are positive odd integers, $n > m, and \; (m, n) = 1$.

Note: If we take $n = 3 \; and \; m = 1$, we get the solution

$$(x, y, z) = (27, 364, 365).$$

Q# 9:

<u>Part (a):</u> Let $F(n) = \sum_{d|n} \frac{\mu(d)}{d^2}$. Then $F(1) = 1$.

Since μ and $g(n) = \frac{1}{n^2}$ are multiplicative functions, then F is a multiplicative function. We thus start by computing F at a prime power p^k ($p \; is \; prime \; and \; k \geq 1$ an integer):

$$F(p^k) = \sum_{d|p^k} \frac{\mu(d)}{d^2} = \sum_{i=0}^{k} \frac{\mu(p^i)}{p^{2i}} = 1 - \frac{1}{p^2}.$$

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

$$F(n) = \prod_{i=1}^{r} F\left(p_i^{\alpha_i}\right) = \prod_{i=1}^{r} \left(1 - \frac{1}{p_i^2}\right) = \prod_{p|n} \left(1 - \frac{1}{p^2}\right).$$

<u>Part (b):</u> If $\sum_{d|n} df(d) = n^2$, then by Mobius Inversion Formula, we get

$$nf(n) = \sum_{d|n} \mu(d) \cdot \left(\frac{n}{d}\right)^2 = n^2 \sum_{d|n} \frac{\mu(d)}{d^2}.$$

Using Part (a), we get

$$f(n) = n \cdot \prod_{p|n} \left(1 - \frac{1}{p^2}\right).$$

Since $1 - \frac{1}{p^2} = \left(1 - \frac{1}{p}\right)\left(1 + \frac{1}{p}\right)$, then we get

$$f(n) = \phi(n) \cdot \prod_{p|n} \left(1 + \frac{1}{p}\right).$$

Q# 10: Completing the square in y, we get

$$(y+3)^2 - x^2 = 3.$$

Factoring, we obtain

$$(y+3-x)(y+3+x) = 3.$$

This gives the following four possibilities:

$$\begin{cases} y+3-x = \pm 1, \pm 3 \\ y+3+x = \pm 3, \pm 1 \end{cases}$$

Solving the four systems, we get the following four solutions

$$(x, y) = (-1, -5), (-1, -1), (1, -5), (1, -1).$$

Q# 11: Note first that $396 = 4 \cdot 9 \cdot 11$. If $(n, 396) = 1$, then $(n, 4) = (n, 9) = (n, 11) = 1$. By using Euler's theorem, we get

$$n^2 \equiv 1 \; mod \; 4 \xRightarrow{15th \; power} n^{30} \equiv 1 \; mod \; 4$$

$$n^6 \equiv 1 \; mod \; 9 \xRightarrow{5th \; power} n^{30} \equiv 1 \; mod \; 9$$

$$n^{10} \equiv 1 \; mod \; 11 \xRightarrow{3rd \; power} n^{30} \equiv 1 \; mod \; 11$$

This implies $n^{30} \equiv 1 \, mod[4,9,11], or \; n^{30} \equiv 1 \, mod \, 396$, and hence $396 | n^{30} - 1$.

Q# 12: Note first that $a\bar{a} \equiv 1 \, mod \, p$. From the properties of Legendre symbol, we get

$$\left(\frac{a\bar{a}}{p}\right) = \left(\frac{1}{p}\right).$$

This implies that

$$\left(\frac{a}{p}\right)\left(\frac{\bar{a}}{p}\right) = 1 \cdots\cdots (*)$$

The proof proceeds as follows:

$$a \; is \; q.r. mod \; p \overset{def}{\Longleftrightarrow} \left(\frac{a}{p}\right) = 1 \overset{(*)}{\Leftrightarrow} \left(\frac{\bar{a}}{p}\right) = 1 \overset{def}{\Longleftrightarrow} \bar{a} \; is \; q.r. mod \; p.$$

Q# 13: Let p be a prime. To show that $(n!)!/(n!)^{(n-1)!}$ is an integer, it is enough to show that if $p^{\gamma} \| \frac{(n!)!}{(n!)^{(n-1)!}}$, then $\gamma \geq 0$.

Let $\alpha_p \; and \; \beta_p$ be nonnegative integers such that $p^{\alpha_p} \| (n!)!$ and $p^{\beta_p} \| (n!)^{(n-1)!}$. Then

$$\alpha_p = \sum_{i=1}^{\infty} \left[\!\left[\frac{n!}{p^i}\right]\!\right]; \; \beta_p = \sum_{i=1}^{\infty} (n-1)! \left[\!\left[\frac{n}{p^i}\right]\!\right].$$

As $[\![x]\!][\![y]\!] \leq [\![xy]\!] \; for \; x \geq 0 \; and \; y \geq 0$, then

$$(n-1)! \left[\!\left[n/p^i\right]\!\right] = [\![(n-1)!]\!] \left[\!\left[n/p^i\right]\!\right] \leq \left[\!\left[\frac{n!}{p^i}\right]\!\right].$$

This implies that

$$\beta_p = \sum_{i=1}^{\infty} (n-1)! \left[\!\left[\frac{n}{p^i}\right]\!\right] \leq \sum_{i=1}^{\infty} \left[\!\left[\frac{n!}{p^i}\right]\!\right] = \alpha_p.$$

Now as $p^{\alpha_p - \beta_p} \| (n!)!/(n!)^{(n-1)!}$ and $\alpha_p - \beta_p \geq 0$, then $\frac{(n!)!}{(n!)^{(n-1)!}}$ is an integer.

Q# 14:

Part (a): We have to show that $\sigma(2p^k) < 4p^k$. As $k \geq 1$ *and* $p \geq 5$, then $(2, p^k) = 1$ and so

$$\sigma(2p^k) = \sigma(2)\sigma(p^k) = 3 \cdot \frac{p^{k+1} - 1}{p - 1} = 3p^k \cdot \frac{p - \left(\frac{1}{p^k}\right)}{p - 1}$$

$$< 3p^k \cdot \frac{p}{p-1} = p^k \cdot \frac{3p}{p-1}.$$

Since $p \geq 5 > 4$, then $\frac{3p}{p-1} < 4$ as

$$\frac{3p}{p-1} < 4 \Leftrightarrow 3p < 4p - 4 \Leftrightarrow 4 < p$$

We conclude that $\sigma(2p^k) < 4p^k$ and hence $2p^k$ is a deficient number for any prime $p \geq 5$ and any integer $k \geq 1$.

Part (b): Note first that when $k = 1$, then 6 is a perfect number ($\sigma(6) = 12 = 2 \cdot 6.$) Assume $k \geq 2$. As $(2, 3^k) = 1$, then

$$\sigma(2 \cdot 3^k) = \sigma(2)\sigma(3^k) = 3 \cdot \frac{3^{k+1} - 1}{3 - 1} = 3 \cdot 3^{k+1} \cdot \frac{1 - \left(\frac{1}{3^{k+1}}\right)}{2}$$

$$= 3^k \cdot \frac{9}{2} \cdot \left(1 - \frac{1}{3^{k+1}}\right) = 4 \cdot 3^k \cdot \frac{9}{8} \cdot \left(1 - \frac{1}{3^{k+1}}\right).$$

Note that

$$k \geq 2 \Rightarrow 3^{k+1} \geq 3^3 = 27 \Rightarrow \frac{1}{3^{k+1}} \leq \frac{1}{27} \Rightarrow 1 - \frac{1}{3^{k+1}} \geq \frac{26}{27}.$$

This implies

$$\frac{9}{8} \cdot \left(1 - \frac{1}{3^{k+1}}\right) \geq \frac{9}{8} \cdot \frac{26}{27} = \frac{13}{12} > 1.$$

We then conclude that $\sigma(2 \cdot 3^k) > 4 \cdot 3^k$ and so $2 \cdot 3^k$ is abundant when $k \geq 2$.

Q# 15: Note first that $q = \frac{p-1}{2}$. Let $h = ord_p(2)$. Then $h|p-1$, or $h|2q$. Thus the possible values of h are

$$h = 1, 2, q, 2q.$$

If $h = 1$, then $2^1 \equiv 1 \; mod \; p$ and hence $p|1$, which is not possible.

If $h = 2$, then $2^2 \equiv 1 \; mod \; p$ and hence $p|3$. This implies that $p = 3$, which is not possible ($n \geq 1 \Rightarrow p = 8n + 3 \geq 11.$)

If $h = q$, then $2^q \equiv 1 \; mod \; p \; or \; 2^{\frac{p-1}{2}} \equiv 1 \; mod \; p$. By Euler's criterion, we get

$$\left(\frac{2}{p}\right) \equiv 1 \; mod \; p.$$

This implies that $\left(\frac{2}{p}\right) = 1$ and hence $p \equiv 1, 7 \; mod \; 8$, which is not possible since $p = 8n + 3 \equiv 3 \; mod \; 8$.

We must then have $h = 2q = p - 1$; i.e., $ord_p(2) = p - 1 = \phi(p)$ and so 2 is a primitive root modulo p.