King Fahd University of Petroleum & Minerals

Department of Mathematics & Statistics

Math 427, Exam I, Term 181

Part I (50 points)

1. **[10 points]** Find $(6327, 962)$ and express it as a linear combination of 6327 and 962.
2. **[10 points]** Let $n \geq 3$ be an integer and let $a_n = \binom{n}{2}$ and $b_n = \binom{n}{3}$. Find (a_n, b_n).
3. **[10 points]** Use Fermat's factorization method to find, if possible, two nontrivial factors of the number 25273.
4. **[10 points]** Find all integer solutions (x, y) of the equation $13x + 7y = 2$ such that $3|x$ and $5|y$.
5. **[10 points]** Find the remainder when Fermat number $F_{100} = 2^{2^{100}} + 1$ is divided by 11.

Part II (50 points)

6. **[10 points]** Let a, b, c be positive integers. Prove that

$$a \left| bc \text{ if and only if } \frac{a}{(a,b)} \right| c.$$

7. **[8 points]** Prove that every prime of the form $5k + 1$ is either of the form $20l + 1$ or of the form $20l + 11$.
8. **[10 points]** Let a, b, c be positive integers. Prove that

$$([a,b],[a,c],[b,c]) = [(a,b),(a,c),(b,c)].$$

9. **[10 points]** Let $R = \{r_1, r_2, \cdots, r_m\}$ and $S = \{s_1, s_2, \cdots, s_n\}$ be two complete residue systems modulo m and n, $respectively$. Let

$$T = \{nr_i + ms_j : 1 \leq i \leq m, 1 \leq j \leq n\}$$

Prove that if $(m, n) = 1$, then the set T is a complete residue system modulo mn.

10. [12 points] Let $p \geq 3$ be a prime number. Prove that

$$\binom{3p}{2p} \equiv 3 \; mod \; p.$$

All the best,

Ibrahim Al-Rasasi

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

Q1: We apply the Euclidean algorithm:

$$6327 = 962(6) + 555$$

$$962 = 555(1) + 407$$

$$555 = 407(1) + 148$$

$$407 = 148(2) + 111$$

$$148 = 111(1) + 37$$

$$111 = 37(3)$$

Thus $(6327,962) = 37$. To write the answer as a linear combination of 6327 and 962, we solve backward for the remainders:

$$37 = (6327,962) = 148 - 111(1) = 148 - [407 - 148(2)]$$

$$= 148(3) - 407 = [555 - 407(1)](3) - 407 = 555(3) - 407(4)$$

$$= 555(3) - [962 - 555(1)](4) = 555(7) - 962(4)$$

$$= [6327 - 962(6)](7) - 962(4) = 6327(7) - 962(46).$$

Thus

$$37 = (6327,962) = 6327(7) + 962(-46).$$

Q2: Note first that $a_n = \frac{n(n-1)}{2}$ and $b_n = \frac{n(n-1)(n-2)}{6}$. Let $g_n = (a_n, b_n)$. To avoid fractions, note that

$$6g_n = \big(3n(n-1), n(n-1)(n-2)\big) = n(n-1)(3, n-2).$$

Now if $n = 3k, k \geq 1, then\ (3, n-2) = (3,3k-2) = 1$,

if $n = 3k+1, k \geq 1, then\ (3, n-2) = (3,3k-1) = 1$, and if $n = 3k + 2, k \geq 1, then\ (3, n - 2) = (3,3k) = 3.$

Thus

$$g_n = \begin{cases} \frac{n(n-1)}{6} & if\ n = 3k\ or\ n = 3k + 1 \\ \frac{n(n-1)}{2} & if\ n = 3k + 2 \end{cases}$$

Here $k \geq 1$ is an integer.

Q3: Let $n = 25273$. Then $\sqrt{n} \approx 158.975$. Thus we start by taking $x = 159$.

$$x = 159 \Rightarrow 159^2 - n = 8(not\ a\ squar)$$

$$x = 160 \Rightarrow 160^2 - n = 327(not\ a\ squar)$$

$$x = 161 \Rightarrow 161^2 - n = 648(not\ a\ squar)$$

$$x = 162 \Rightarrow 162^2 - n = 971(not\ a\ squar)$$

$$x = 163 \Rightarrow 163^2 - n = 1296 = 36^2.$$

Thus

$$n = 163^2 - 36^2 = (163 - 36)(163 + 36) = 127 \cdot 199.$$

In fact, both factors 127 and 199 are primes and so we get a complete factorization.

Q4: Since $3|x\ and\ 5|y, then\ x = 3z\ and\ y = 5w$. The equation becomes

$$39z + 35w = 2.$$

As $(39,35) = 1$ divides 2, then the equation is solvable in integers. Using the Euclidean algorithm (three steps of division), we find that $(z, w) = (18, -20)$ is a solution and hence the solutions are

$$z = 18 + 35t, \qquad w = -20 - 39t, t \in \mathbb{Z}.$$

This implies that the required solutions are

$$x = 54 + 105t, \qquad w = -100 - 195t, \qquad t \in \mathbb{Z}.$$

Q5: We need to find an integer r such that

$$F_{100} = 2^{2^{100}} + 1 \equiv r \; mod \; 11, \qquad 0 \leq r \leq 10.$$

By Fermat's Theorem,

$$2^{10} \equiv 1 \; mod \; 11.$$

We divide 2^{100} by 10. For this, note first that

$$2^5 \equiv 2 \; mod 10.$$

This implies that

$$2^{100} \equiv 2^{20} \equiv 2^4 \equiv 6 \; mod 10.$$

Thus $2^{100} = 6 + 10q$, for some positive integer q. We get

$$2^{2^{100}} = 2^{10q+6} = (2^{10})^q \cdot 2^6 \equiv 1^q \cdot (-2) \equiv -2 \; mod \; 11$$

This implies that

$$F_{100} \equiv -1 \equiv 10 \; mod \; 11.$$

We conclude that the remainder when F_{100} is divided by 11 is 10.

Q6: Let $(a, b) = g$. Then $\left(\frac{a}{g}, \frac{b}{g}\right) = 1$.

⇒: Assume $a|bc$. Then $bc = ak$ for some positive integer k. Dividing by g, we get $\frac{b}{g}c = \frac{a}{g}k$. Since $\frac{a}{g} | \frac{b}{g}c \ and \ \left(\frac{a}{g}, \frac{b}{g}\right) = 1$, then $\frac{a}{g}\Big|c; i.e., \frac{a}{(a,b)}\Big| c$.

⇐: Assume $\frac{a}{(a,b)}|c$. We also have $(a,b)|b$. Multiplying, we get

$$\frac{a}{(a,b)} \cdot (a,b)|cb; or\ a|bc.$$

Q7: Any integer k takes one of the following forms: $4l, 4l+1, 4l+2, or\ 4l+3$. Thus any integer of the form $5k+1$ takes one of the following forms:

$$5(4l)+1 = 20l+1,$$

$$5(4l+1)+1 = 20l+6,$$

$$5(4l+2)+1 = 20l+11,$$

$$5(4l+3)+1 = 20l+16.$$

Now $20l+6\ and\ 20l+16$ are composite (divisible respectively by 2 and 4.) Then any **prime** number of the form $5k+1$ will take one of the forms $20l+1\ or\ 20l+11$.

Q8: To prove equality, it is enough, by the Fundamental Theorem of Arithmetic, to show that each prime is raised to the same power in both sides. Let p be a prime and let the powers of p in $a, b, and\ c$ be $\alpha, \beta, and\ \gamma, respectively$. Without loss of generality, we may assume $\alpha \le \beta \le \gamma$.

Now the powers of p in $[a,b], [a,c], and\ [b,c]$ are $\beta, \gamma, and\ \gamma, respectively$. So the power of p in $([a,b],[a,c],[b,c])$ is β.

Also the powers of p in $(a,b),(a,c), and\ (b,c)$ are $\alpha,\alpha, and\ \beta, respectively$. So the power of p in $[(a,b),(a,c),(b,c)]$ is β. Since the power of p in both sides is the same, equality holds.

Q9: The set T contains mn elements. So to show that T is a complete residue system modulo mn, it is enough to show that no two distinct elements of T are congruent modulo mn.

Assume two distinct elements of T are congruent modulo mn:

$$nr_i + ms_j \equiv nr_k + ms_l \ mod\ mn \cdots\cdots (*)$$

where $1 \le i,k \le \phi(m), 1 \le j,l \le \phi(n)$. Since $m|mn$, the last congruence reduces to

$$nr_i + ms_j \equiv nr_k + ms_l \ mod\ m$$

or,

$$nr_i \equiv nr_k \ mod\ m$$

As $(m,n) = 1$, we get $r_i \equiv r_k \ mod\ m$. If $i \ne k$, we get a contradiction (R is a complete residue system modulo m: no two different elements of R are congruent modulo m.) So suppose that $i = k$. Substituting in $(*)$ and simplifying, we get $ms_j \equiv ms_l \ mod\ mn$. Cancelling m, we get $s_j \equiv s_l \ mod\ n$. But since $j \ne l$ (as the two elements we started with are distinct and $i = k$), we get a contradiction (S is a complete residue system modulo n: no two different elements of S are congruent modulo n.)

Because of this contradiction, we conclude that no two distinct elements of T are congruent modulo mn and hence T is a complete residue system modulo mn.

Q10: Let $p \geq 3$ be prime. Note first that

$$\binom{3p}{2p} = \frac{(3p)!}{(2p)! \cdot p!} = \frac{(3p)(3p-1)(3p-2)\cdots(2p+1)}{p!}$$

$$= \frac{3(3p-1)(3p-2)\cdots\big(3p-(p-1)\big)}{(p-1)!}$$

Avoiding fractions, we get

$$(p-1)! \cdot \binom{3p}{2p} = 3(3p-1)(3p-2)\cdots\big(3p-(p-1)\big).$$

Now we compute modulo p:

$$(p-1)! \cdot \binom{3p}{2p} \equiv 3(-1)(-2)\cdots\big(-(p-1)\big)\, mod\ p$$

$$\equiv 3 \cdot (p-1)!\, mod\ p.$$

As ($\big((p-1)!, p\big) = 1$, we can cancel $(p-1)!$ to obtain

$$\binom{3p}{2p} \equiv 3\ mod\ p.$$