KFUPM

Department of Mathematics

Math 427, Exam I, Term 242.

<u>Part I (50 points)</u>

1. **[10 points]** Find all integers n such that $5n+3|7n+3$.
2. **[10 points]** Use Fermat's Factorization method to find, if possible, two nontrivial factors of the number 846319.
3. **[10 points]** Solve $2025x-1446y=6$ in integers.
4. **[10 points]** Find the remainder when Fermat Number $F_{100}=2^{2^{100}}+1$ is divided by 7.
5. **[10 points]** Determine whether or not $70=2\cdot 5\cdot 7$ is a pseudoprime to the base 11.

<u>Part II (50 points)</u>

6. **[10 points]** Prove that $n+1|\binom{2n}{n}$ for any integer $n\geq 1$.
7. **[10 points]** Let $a\ and\ b$ be positive integers. Let $[a,b]=m$ and write $m=a\alpha$ and $m=b\beta$ for some positive integers $\alpha\ and\ \beta$. Prove that $(\alpha,\beta)=1$.
8. **[10 points]** Prove that the following fraction is in lowest form for any integer n:

$$\frac{n^2+n-1}{2n^3+n^2-n+1}.$$

9. **[10 points]** Let $p\geq 3$ be a prime number. Prove that $p|(p-3)!+2^{p-2}$. **Hint:** Use Wilson's Theorem and Fermat's Theorem.
10. **[10 points]** Let $r_1,r_2,\cdots,r_{p-1}$ be a reduced residue system modulo a prime $p\geq 3$. Prove that

$$p|r_1+r_2+\cdots+r_{p-1}.$$

Good luck,

Ibrahim Al-Rasasi

Solutions

Q1: Find all integers n such that $5n + 3 | 7n + 3$.

Solution: Note that $7 \cdot (5n + 3) - 5 \cdot (7n + 3) = 6$. Then $5n + 3 | 7n + 3$ if and only if $5n + 3 | 6$. This implies that $5n + 3 = \pm 1 \; or \; \pm 2 \; or \; \pm 3 \; or \; \pm 6$. Solving, we conclude that the only possible integers are $n = -1$ and $n = 0$.

Q2: Use Fermat's Factorization method to find, if possible, two nontrivial factors of the number 846319.

Solution: As $\sqrt{846319} \approx 919.56$, we start by taking $x = 920, 921, 922, \cdots$.

Now

$$x^2 - 846319 = 920^2 - 846319 = 81 = 9^2, \text{ a square.}$$

Then $846319 = 920^2 - 9^2 = (920 - 9)(920 + 9) = 911 \times 929$.

Q3: Solve $2025x - 1446y = 6$ in integers.

Solution: We use the Euclidean algorithm to find $(2025, 1446)$:

$$2025 = 1446\,(1) + 579,$$

$$1446 = 579(2) + 288,$$

$$579 = 288(2) + 3,$$

$$288 = 3(96).$$

Thus $(2025, 1446) = 3$ and $3|6$ and hence the equation is solvable. Solving backward for the remainders we find that

$$3 = 2025(5) - 1446(7).$$

Multiplying by 2, we get

$$6 = 2025(10) - 1446(14).$$

Thus $(x_0, y_0) = (10, 14)$ is one solution of the equation. All other solutions are

$$x = 10 + \left(\frac{1446}{3}\right)t = 10 + 482t, y = 14 + \left(\frac{2025}{3}\right)t = 14 + 675t, t \in \mathbb{Z}.$$

Q4: Find the remainder when Fermat Number $F_{100} = 2^{2^{100}} + 1$ is divided by 7.

Solution: Note that $2^3 \equiv 1 \ mod\ 7$. Next we divide 2^{100} by 3: $2^{100} = 3q + r$. Using congruences, $2 \equiv -1 \ mod\ 3$ and so $2^{100} \equiv 1 \ mod\ 3$. This implies that $2^{100} = 1 + 3q$ for some positive integer q. Now we have:

$$2^3 \equiv 1 \ mod\ 7 \Rightarrow 2^{3q} \equiv 1 \ mod\ 7 \Rightarrow 2^{3q+1} \equiv 2 \ mod\ 7$$

$$\Rightarrow 2^{2^{100}} \equiv 2 \ mod\ 7 \Rightarrow F_{100} \equiv 3 \ mod\ 7.$$

We conclude that the required remainder is 3.

Q5: Determine whether or not 70 is a pseudoprime to the base 11.

Solution: We need to check whether or not $11^{69} \equiv 1 \ mod\ 70$. As $70 = 2 \cdot 5 \cdot 7$, we have first to compute 11^{69} modulo 2, 5, and 7.

Since $11 \equiv 1 \ mod\ 2$, then $11^{69} \equiv 1 \ mod\ 2$.

By Fermat's Theorem, $11^4 \equiv 1 \ mod\ 5$. As $69 = 4 \cdot 17 + 1 = 68 + 1$, then raising to the 17th power, we get $11^{68} \equiv 1 \ mod\ 5$, and multiplying by 11, we get $11^{69} \equiv 11 \ mod\ 5$. But $11 \equiv 1 \ mod\ 5$. Then $11^{69} \equiv 1 \ mod\ 5$.

Again, by Fermat's Theorem, $11^6 \equiv 1 \ mod\ 7$. As $69 = 6 \cdot 11 + 3 = 66 + 3$, then raising to the 11th power, we get $11^{66} \equiv 1 \ mod\ 7$, and multiplying by 11^3, we get $11^{69} \equiv 11^3 \ mod\ 7$. But $11^3 \equiv 4^3 = 8 \cdot 8 \equiv 1 \cdot 1 = 1 \ mod\ 7$. Then $11^{69} \equiv 1 \ mod\ 7$.

Now since $11^{69} \equiv 1 \ mod\ 2, 11^{69} \equiv 1 \ mod\ 5, and\ 11^{69} \equiv 1 \ mod\ 7$, then

$$11^{69} \equiv 1 \ mod\ [2, 5, 7],$$

and hence $11^{69} \equiv 1 \ mod\ 70$. We conclude that 70 is a pseudoprime to the base 11.

Q6: Prove that $n+1|\binom{2n}{n}$ for any integer $n \geq 1$.

Solution: Note that

$$\binom{2n}{n} = \frac{(2n)!}{n! \cdot n!} = \frac{(n+1)\cdot(n+2)\cdot\cdots(2n-1)\cdot(2n)}{n!}$$
$$= \frac{(n+1)\cdot(n+2)\cdot\cdots(2n-1)\cdot(2n)}{n\cdot(n-1)!}$$
$$= \frac{n+1}{n}\cdot\frac{(n+2)\cdot\cdots(2n-1)\cdot(2n)}{(n-1)!} = \frac{n+1}{n}\cdot a,$$

where a is some integer (the product of $n-1$ consecutive integers is divisible by $(n-1)!$). This can be written as

$$n\cdot\binom{2n}{n} = (n+1)\cdot a.$$

As $n+1|n\cdot\binom{2n}{n}$ and $(n+1,n)=1$, then $n+1|\binom{2n}{n}$.

Q7: Let $a \; and \; b$ be positive integers. Let $[a,b]=m$ and write $m=a\alpha$ and $m=b\beta$ for some positive integers $\alpha \; and \; \beta$. Prove that $(\alpha,\beta)=1$.

Solution: Let $(a,b)=d$. As $[a,b](a,b)=ab$, then $md=ab$. This implies that

$$a\alpha d = ab \Rightarrow \alpha d = b,$$

$$b\beta d = ab \Rightarrow \beta d = a.$$

Now $d=(a,b)=(\beta d,\alpha d)=d(\beta,\alpha)$ and hence $(\alpha,\beta)=1$.

Q8: Prove that the following fraction is in lowest form for any integer n:

$$\frac{n^2+n-1}{2n^3+n^2-n+1}.$$

Solution: We need to show that $(2n^3+n^2-n+1,\ n^2+n-1)=1$. By dividing we get

$$2n^3 + n^2 - n + 1 = (n^2 + n - 1)(2n - 1) + 2n.$$

This implies that

$$(2n^3 + n^2 - n + 1, \qquad n^2 + n - 1) = (n^2 + n - 1, \qquad 2n).$$

Let $(n^2 + n - 1,\ 2n) = g$. As

$$2(n^2 + n - 1) - (2n)(n + 1) = -2,$$

then $g|2$ and hence either $g = 1\ or\ g = 2$. But $n^2 + n - 1 = n(n + 1) - 1$ is odd (as $n(n + 1)$ is even). Then $g = 1$ and so the given fraction is in lowest form.

Q9: Let $p \geq 3$ be a prime number. Prove that $p|(p - 3)! + 2^{p-2}$. **Hint:** Use Wilson's Theorem and Fermat's Theorem.

Solution: By Wilson's Theorem, $(p - 1)! \equiv -1\ mod\ p$ implies that

$$(p - 1)(p - 2) \cdot (p - 3)! \equiv -1\ mod\ p$$

and hence $(-1)(-2) \cdot (p - 3)! \equiv -1\ mod\ p$, or

$$2 \cdot (p - 3)! \equiv -1\ mod\ p.$$

Multiplying both sides by 2^{p-2} gives $2^{p-1} \cdot (p - 3)! \equiv -2^{p-2}\ mod\ p$. But, by Fermat's Theorem, $2^{p-1} \equiv 1\ mod\ p$. So the last congruence reduces to

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

and so $p|(p - 3)! + 2^{p-2}$.

Q10: Let $r_1, r_2, \cdots, r_{p-1}$ be a reduced residue system modulo a prime $p \geq 3$. Prove that

$$p|r_1 + r_2 + \cdots + r_{p-1}.$$

Solution: We are given that the set $T = \{r_1, r_2, \cdots, r_{p-1}\}$ is a RRS_p. Note first that the set $S = \{1, 2, \cdots, p - 1\}$ is a RRS_p. Thus every element of T is congruent to one element of S, and no two elements of T are congruent to the same element of S:

If $r_i \equiv a \, mod \, p$ and $r_j \equiv a \, mod \, p$, where $1 \leq i < j \leq p-1$ and $1 \leq a \leq p-1$, then $r_i \equiv r_j \, mod \, p$, contradicting the given assumption that the set T is a RRS_p.

This implies that there is a one-to-one correspondence (via $\equiv$) between the elements of T and the elements of S:

$$\{r_1, r_2, \cdots, r_{p-1}\} \overset{\equiv}{\leftrightarrow} \{1, 2, \cdots, p-1\}.$$

(Not necessarily in the same order). Thus, we have

$$r_1 + r_2 + \cdots + r_{p-1} \equiv 1 + 2 + \cdots + (p-1) \, mod \, p.$$

Since $1 + 2 + \cdots + (p-1) = \frac{p-1}{2} p$ and $\frac{p-1}{2}$ is an integer, then

$$1 + 2 + \cdots + (p-1) \equiv 0 \, mod \, p,$$

and hence

$$r_1 + r_2 + \cdots + r_{p-1} \equiv 0 \, mod \, p,$$

which is the same thing as $p | r_1 + r_2 + \cdots + r_{p-1}$.