Problem 1. Prove that $a \equiv b \pmod{c}$ if and only if a and b give the same remainders upon division by c.

Solution: Let r_a, r_b be the remainders of a, b upon division by c respectively. Thus $a \equiv r_a \pmod{c}$ and $b \equiv r_b \pmod{c}$. It follows that $a \equiv b \pmod{c}$ iff $r_a \equiv r_b \pmod{c}$, i.e. iff $c|(r_a - r_b)$. Note that $0 \leq r_a, r_b < c$, so $|r_a - r_b| < c$. Thus the only way for $c|(r_a - r_b)$ to hold is to have $r_a = r_b$.

Problem 2. a) Find the remainder upon division of 2^{85} by 341.

b) Find smallest $a > 0$ such that $2^a \equiv 1 \pmod{341}$.

Solution: a) Use succesive squarings. We have $85 = 2^6 + 2^4 + 2^2 + 2^0$.

$$2^{2^0} \equiv 2 \pmod{341} ,$$

$$2^{2^1} \equiv 4 \pmod{341} ,$$

$$2^{2^2} \equiv 16 \pmod{341} ,$$

$$2^{2^3} \equiv 16^2 \equiv 256 \equiv -85 \pmod{341} ,$$

$$2^{2^4} \equiv (-85)^2 \equiv 64 \pmod{341} ,$$

$$2^{2^5} \equiv 64^2 \equiv 4 \pmod{341} ,$$

$$2^{2^6} \equiv 4^2 = 16 \pmod{341} ,$$

Thus

$$2^{85} = 2^{2^6} \cdot 2^{2^4} \cdot 2^{2^2} \cdot 2^{2^0} \equiv 16 \cdot 64 \cdot 16 \cdot 2 = 2^{2^3} \cdot 2^7 \equiv (-85) \cdot 4 \cdot 2^5 \equiv (-340) \cdot 2^5 \equiv 2^5 \pmod{341}$$

b) Note that from a) we have $2^8 \equiv -85 \pmod{341}$. Since $4 \cdot 85 = 340$, we have

$$2^{10} = 2^8 \cdot 4 \equiv (-85) \cdot 4 = -340 \equiv 1 \pmod{341} .$$

Since $2^8 < 341$ and $2^9 = 512 \not\equiv 1 \pmod{341}$, $a = 10$ is the smallest positive integer such that $2^a \equiv 1 \pmod{341}$.

Problem 3. For positive integers a, b define $[a, b] = ab/\gcd(a, b)$.

a) Prove that $a/\gcd(a, b)$ and $b/\gcd(a, b)$ are relatively prime.

b) Prove that if $a|c$ and $b|c$ then $[a, b]|c$.

c) Conlcude that $[a, b]$ is the smallest positive integer divisible by both a and b (we call it the **least common multiple of** a **and** b).

Solution: a) If $d > 0$ is a common divisor of $a/\gcd(a, b)$ and $b/\gcd(a, b)$ then $d \gcd(a, b)$ divides both a and b and hence $d \gcd(a, b) \leq \gcd(a, b)$. It follows that $d \leq 1$, i.e. $d = 1$. In other words, $a/\gcd(a, b)$ and $b/\gcd(a, b)$ do not have any positive common divisors different from 1, i.e. they are relatively prime.

b) Note that $a|c$ implies that $\frac{a}{\gcd(a,b)}|\frac{c}{\gcd(a,b)}$. Similarly, $\frac{b}{\gcd(a,b)}|\frac{c}{\gcd(a,b)}$. Since by a) the numbers $a/\gcd(a,b)$ and $b/\gcd(a,b)$ are relatively prime, we conclude that their product also divides $c/\gcd(a,b)$. In other words $\frac{ab}{\gcd(a,b)^2}|\frac{c}{\gcd(a,b)}$. It follows that $[a,b]=\frac{ab}{\gcd(a,b)}|c$.

c) Clearly $[a,b]$ is divisible by both a and b. On the other hand, any positive integer divisible by both a and b is according to b) also divisible by $[a,b]$, hence it can not be smaller than $[a,b]$. It means that $[a,b]$ is the lest common multiple of a and b.

Problem 4. Let $F_n = 2^{2^n}+1$, for $n=0,1,2,....$

a) Prove that $F_0 \cdot F_1 \cdot F_2 \cdot ... \cdot F_n = F_{n+1}-2$ for every n.

b) Prove that $\gcd(F_n,F_m)=1$ for $n \neq m$.

c) Use b) to prove that the set of primes is infinite.

Solution: a) The easiest proof seems to be by induction on n. Since $F_0 = 3 = 5-2 = F_1-2$, the result holds for $n=0$. Suppose that it holds for some $n \geq 0$, i.e.

$$F_0 \cdot F_1 \cdot F_2 \cdot ... \cdot F_n = F_{n+1}-2 = 2^{2^{n+1}}-1.$$

Multiplying both sides by $F_{n+1} = 2^{2^{n+1}}+1$ we get

$$F_0 \cdot F_1 \cdot F_2 \cdot ... \cdot F_n \cdot F_{n+1} = (2^{2^{n+1}}-1)(2^{2^{n+1}}+1) = 2^{2^{n+2}}-1 = F_{n+2}-2.$$

so the result holds for $n+1$. By induction, it holds for every $n \geq 0$.

b) Suppose that $m<n$ and d is the greatest common divisor of F_m and F_n. Clearly d divides $F_0 \cdot F_1 \cdot F_2 \cdot ... \cdot F_{n-1}$ (since F_m is one of the factors) and therefore it divides the difference $F_n - F_0 \cdot F_1 \cdot F_2 \cdot ... \cdot F_{n-1}$, which is 2 by a). Thus $d|2$, i.e. $d=1$ or $d=2$. Hovewer $d=2$ is not possible, since the numbers F_k are all odd. Hence $d=1$, i.e. $\gcd(F_n,F_m)=1$.

c) Each number F_n has at least one prime divisor. Choose any one of them and call it p_n. Since $\gcd(F_n,F_m)=1$, we have $p_n \neq p_m$ if $n \neq m$. Thus $p_1, p_2, \ldots$ is an infinite list of pairwise different primes.

Problem 5. Let a be a number written (in base 10) as

$$a = a_0 + a_1 \cdot 10 + a_2 \cdot 10^2 + ... + a_n \cdot 10^n,$$

where $0 \leq a_i < 10$.

(i) Prove that $a \equiv a_0 \pmod 2$. In particular, $2|a$ iff $2|a_0$.

(ii) Prove that $a \equiv a_0 + 2a_1 \pmod 4$. In particular, $4|a$ iff $4|a_0+2a_1$.

(iii) Prove that $a \equiv a_0 + 2a_1 + 4a_2 \pmod 8$. In particular, $8|a$ iff $8|a_0+2a_1+4a_2$.

(iv) Prove that $a \equiv a_0 \pmod 5$. In particular, $5|a$ iff $5|a_0$.

(v) Prove that $a \equiv a_0+a_1+\ldots+a_n \pmod 9$. In particular, $9|a$ iff $9|\ a_0+a_1+\ldots+a_n$.

(vi) Prove that $a \equiv a_0 + a_1 + \ldots + a_n \pmod 3$. In particular, $3|a$ iff $3|\ a_0 + a_1 + \ldots + a_n$.

(vii) Prove that $a \equiv a_0 - a_1 + a_2 - \ldots \pmod{11}$. In particular, $11 \mid a$ iff $11|\ a_0 - a_1 + a_2 - \ldots$.

Solution: Let $a = a_0 + a_1 \cdot 10 + a_2 \cdot 10^2 + ... + a_n \cdot 10^n$.

Since $10^k \equiv 0 \pmod 2$ for $k > 0$ we see that

$$a \equiv a_0 \pmod 2 .$$

Thus $2|a$ iff $2|a_0$.

Similarly, $10^k \equiv 0 \pmod 5$ for $k > 0$ so

$$a \equiv a_0 \pmod 5 .$$

Thus $5|a$ iff $a_0 = 0$ or $a_0 = 5$ (recall that the numbers a_i are the digits of a, i.e. they all are in the set $\{0, 1, 2, 3, 4, 5, 6, 7, 8, 9\}$).

Now $10 \equiv 2 \pmod 4$ and $10^k \equiv 0 \pmod 4$ for $k \geq 2$ so

$$a \equiv a_0 + a_1 \cdot 10 \equiv a_0 + 2a_1 \pmod 4 .$$

It follows that $4|a$ iff $4|a_0 + 2a_1$.

Similarly, we have $10 \equiv 2 \pmod 8$, $10^2 \equiv 4 \pmod 8$ and $10^k \equiv 0 \pmod 8$ for $k \geq 3$. Thus

$$a \equiv a_0 + a_1 \cdot 10 + a_2 \cdot 10^2 \equiv a_0 + 2a_1 + 4a_2 \pmod 8 .$$

In particular, $8|a$ iff $8|a_0 + 2a_1 + 4a_2$.

Note now that $10 \equiv 1 \pmod 3$ and $10 \equiv 1 \pmod 9$. Thus $10^k \equiv 1 \pmod 3$ and $10^k \equiv 1 \pmod 9$ for every $k \geq 0$. It follows that

$$a \equiv a_1 + a_1 + ... + a_n \pmod 3$$

and

$$a \equiv a_1 + a_1 + ... + a_n \pmod 9 .$$

In particular, $3|a$ iff $3|a_1 + a_1 + ... + a_n$ and $9|a$ iff $9|a_1 + a_1 + ... + a_n$.

Since $10 \equiv -1 \pmod{11}$, we have $10^k \equiv 1 \pmod{11}$ for k even and $10^k \equiv -1 \pmod{11}$ for k odd. Consequently,

$$a \equiv a_0 - a_1 + a_2 - a_3 + ... \pmod{11} .$$

Thus $11|a$ iff $11|a_0 - a_1 + a_2 - a_3 + ...$

Problem 6. Compute $\lambda, \mu \in \mathbb{Z}$ such that $89\lambda + 55\mu = 1$ and find all solutions $x \in \mathbb{Z}$ to $89x \equiv 7 \pmod{55}$.

Solution: We perform Euclidean algorithm to 89 and 55:

$$89 = 55 + 34,$$

$$55 = 34 + 21,$$

$$34 = 21 + 13,$$
$$21 = 13 + 8,$$
$$13 = 8 + 5,$$
$$8 = 5 + 3,$$
$$5 = 3 + 2,$$
$$3 = 2 + 1,$$
$$2 = 2 \cdot 1 + 0.$$

Thus

$$1 = 3-2 = 3-(5-3) = 2\cdot 3-5 = 2(8-5)-5 = 2\cdot 8-3\cdot 5 = 2\cdot 8-3\cdot(13-8) = 5\cdot 8-3\cdot 13 =$$
$$= 5 \cdot (21 - 13) - 3 \cdot 13 = 5 \cdot 21 - 8 \cdot 13 = 5 \cdot 21 - 8 \cdot (34 - 21) = 13 \cdot 21 - 8 \cdot 34 =$$
$$13 \cdot (55 - 34) - 8 \cdot 34 = 13 \cdot 55 - 21 \cdot 34 = 13 \cdot 55 - 21 \cdot (89 - 55) = 34 \cdot 55 - 21 \cdot 89.$$

Thus $\lambda = -21$, $\mu = 34$ work. From $1 = 34 \cdot 55 - 21 \cdot 89$ we see that

$$89 \cdot (-21) \equiv 1 \pmod{55} .$$

Mulyplying this congruence by 7 we get

$$89 \cdot (-21) \cdot 7 \equiv 7 \pmod{55} .$$

To simplyfy, note that $(-21) \cdot 7 = -147 \equiv 18 \pmod{55}$, so

$$89 \cdot 18 \equiv 7 \pmod{55} .$$

Since $(89, 55) = 1$, all solutions are given by $x = 18 + k \cdot 55$, $k \in \mathbb{Z}$.

Problem 7. Solve the system of congruences:

$$x \equiv 17 \pmod{504} , \ x \equiv -4 \pmod{35} , \ x \equiv 33 \pmod{16} .$$

Solution: We are asked to solve the system

$$x \equiv 17 \pmod{504} , \ x \equiv -4 \pmod{35} , \ x \equiv 33 \pmod{16} .$$

Since the moduli are not pairwise relatively prime we can not apply Chinese remainder theorem to this system. Note that $504 = 8 \cdot 9 \cdot 7$ and $35 = 5 \cdot 7$. Now the congruence $x \equiv 17 \pmod{504}$ is equivalent to the three congruences

$$x \equiv 17 \equiv 1 \pmod{8} , \ x \equiv 17 \equiv -1 \pmod{9} , \ x \equiv 17 \equiv 3 \pmod{7} .$$

Similarly, the congruence $x \equiv -4 \pmod{35}$ is equivalent to the system

$$x \equiv -4 \equiv 1 \pmod{5} , \ x \equiv 3 \pmod{7} .$$

Finally the congruence $x \equiv 33 \pmod{16}$ is the same as $x \equiv 1 \pmod{16}$. So our original system is equivalent to the system

$$x \equiv 1 \pmod{16}\ ,\ x \equiv -1 \pmod{9}\ ,\ x \equiv 3 \pmod{7}\ ,\ x \equiv 1 \pmod{5}\ .$$

(note that we did not include $x \equiv 1 \pmod{8}$ since this congruence is a consequence of $x \equiv 1 \pmod{16}$).

Now we may apply Chinese remainder theorem. We calculate that

$$(-59) \cdot 16 + 3 \cdot (9 \cdot 7 \cdot 5) = 1,$$

$$249 \cdot 9 + (-4) \cdot 16 \cdot 7 \cdot 5 = 1,$$

$$103 \cdot 7 + (-1) \cdot 16 \cdot 9 \cdot 5 = 1,$$

$$(-403) \cdot 5 + 2 \cdot (16 \cdot 9 \cdot 7) = 1.$$

A solution to our system is therefore given by

$$x = 3 \cdot (9 \cdot 7 \cdot 5) + (-1) \cdot (-4) \cdot 16 \cdot 7 \cdot 5 + 3 \cdot (-1) \cdot 16 \cdot 9 \cdot 5 + 2 \cdot (16 \cdot 9 \cdot 7) = 3041.$$

All solotions to this sustem are theorefore given by

$$x = 3041 + k \cdot 16 \cdot 9 \cdot 7 \cdot 5 = 3041 + k \cdot 5040,$$

where $k \in \mathbb{Z}$.

Problem 8. An old women goes to market and a horse steps on her basket and crushes her eggs. The rider offers to pay for the damages and asks her how many eggs she had brought. She does not remember the exact number, but when she had taken them out two at a time, there was one egg left at the end. The same thing happened when she picked them out three, four, five, and six at a time, but when she took them out seven at a time, no egg left at the end. What is the smallest number of eggs she could have had?

Solution: The problem asks us to find smalest positive solution to the system of congruences

$$x \equiv 1 \pmod{2}\ ,\ x \equiv 1 \pmod{3}\ ,\ x \equiv 1 \pmod{4}\ ,$$

$$x \equiv 1 \pmod{5}\ ,\ x \equiv 1 \pmod{6}\ ,\ x \equiv 0 \pmod{7}\ .$$

The moduli are not pairwise relatively prime here. Note however that the congruences

$$x \equiv 1 \pmod{3}\ ,\ x \equiv 1 \pmod{4}\ ,\ x \equiv 1 \pmod{5}\ ,\ x \equiv 0 \pmod{7}$$

imply the remaining two congruences. So the latter systm is equivalent to the former. Now the moduli are pairwise relatively prime and we can apply Chinese remainder theorem.

$$47 \cdot 3 + (-1) \cdot 4 \cdot 5 \cdot 7 = 1,$$

$$(-26) \cdot 4 + 3 \cdot 5 \cdot 7 = 1,$$

$$17 \cdot 5 + (-1) \cdot \cdot 3 \cdot 4 \cdot 7 = 1,$$

$$(-17) \cdot 7 + 2 \cdot 3 \cdot 4 \cdot 5 = 1.$$

A solution to our system is given by

$$x = (-1) \cdot 4 \cdot 5 \cdot 7 + 3 \cdot 5 \cdot 7 + (-1) \cdot \cdot 3 \cdot 4 \cdot 7 + 0 \cdot 2 \cdot 3 \cdot 4 \cdot 5 = -119.$$

The smallest positive solution is then $-119 + 3 \cdot 4 \cdot 5 \cdot 7 = 301$.

Problem 9. a) Prove that any natural number n such that $n \equiv 3 \pmod 4$ has a prime divisor p such that $p \equiv 3 \pmod 4$ (hint: note that every odd prime number q either satisfies $q \equiv 1 \pmod 4$ or $q \equiv 3 \pmod 4$; what can you say about product of primes of the first type?)

b) Prove that $n! - 1 \equiv 3 \pmod 4$ for any $n > 3$.

c) Prove that every prime divisor of $n! - 1$ is bigger than n.

d) Conclude that there are infinitely many primes q such that $q \equiv 3 \pmod 4$.

Solution: a) Note that for every odd integer m either $m \equiv 1 \pmod 4$ or $m \equiv 3 \pmod 4$. Also, iff $a_1, ..., a_s$ are integers satisfying $a_i \equiv 1 \pmod 4$ for $i = 1, 2, ..., s$ then by multiplying these congruences we see that $a_1 a_2 ... a_s \equiv 1 \pmod 4$.

Consider now a positive integer $n \equiv 3 \pmod 4$. Note that n is odd, so all its prime divisors are odd. We know that n is a product of prime numbers. If each of these prime numbers were $\equiv 1 \pmod 4$, then according to our remark above, also their product n would be $\equiv 1 \pmod 4$, which is false. Thus n must have a prime divisor $p \equiv 3 \pmod 4$.

b) If $n > 3$ then $n! = 1 \cdot 2 \cdot 3 \cdot ... \cdot n$ is divisible by 4. Thus $n! \equiv 0 \pmod 4$ and $n! - 1 \equiv -1 \equiv 3 \pmod 4$.

c) If $p \leq n$ then p divides $n!$ and therefore does not divide $n! - 1$. It follows that any divisor of $n! - 1$ is larger than n.

d) Let $n > 3$. By a) and b) there is a prime number $q \equiv 3 \pmod 4$ which divides $n! - 1$ and $q > n$ by c). Thus there are arbitrarily large primes $\equiv 3 \pmod 4$, so the set of such primes is infinite.

Problem 10. Prove that every composite number n has a prime divisor not larger than $\sqrt{n}$.

Solution: Since n is composite, we may factor n as $n = ab$, where $1 < a \leq b$. Thus $n = ab \geq a^2$ and $\sqrt{n} \geq a$. Any prime divisor of a is a prime divisor of n and it is $\leq \sqrt{n}$.

Problem 11. The numbers n, $n + 2$, $n + 4$ are prime. What is n? Prove your answer. (Hint: consider these numbers modulo 3).

Solution: Note that one of the congruences $n \equiv 0 \pmod 3$, $n \equiv 1 \pmod 3$, $n \equiv 2 \pmod 3$ holds. If $n \equiv 0 \pmod 3$ then $3|n$. Since n is a prime, we must have $n = 3$ and then indeed $n + 2 = 5$, $n + 4 = 7$ are primes.

If $n \equiv 1 \pmod 3$ then $n + 2 \equiv 3 \equiv 0 \pmod 3$, i.e. $3|n + 2$. Since $n + 2$ is a prime, we must have $3 = n + 2$, i.e. $n = 1$. Hovewer, $n = 1$ is not a prime, so this case is not possible.

If $n \equiv 2 \pmod 3$ then $n+4 \equiv 6 \equiv 0 \pmod 3$, i.e. $3|n+4$. Again, since $n+4$ is prime, we have $n+4=3$, i.e. $n=-1$, which is not possible.

Thus $n=3$ is the only solution.

Problem 12. Use Euler Theorem to find the remainder upon division of n by m, where

a) $n=29^{202}$, $m=13$;

b) $n=99^{999999}$, $m=23$

c) $n=29^{198}$, $m=20$

d) $n=3^{1000000}$, $m=14$

Solution: a) Note that $29 \equiv 3 \pmod{13}$. Thus $29^{202} \equiv 3^{202} \pmod{13}$. It suffices then to find remainder upon division of 3^{202} by 13.

By Euler's theorem (or its special case Fermat's Little Theorem) we have $3^{12} \equiv 1 \pmod{13}$. Now $202 = 12 \cdot 16 + 10$. Thus

$$3^{202} = 3^{12 \cdot 16 + 10} = (3^{12})^{16} \cdot 3^{10} \equiv 3^{10} \pmod{13} .$$

Now $3^{10} = 9^5$ and $9 \equiv -4 \pmod{13}$. Thus

$$3^{10} \equiv (-4)^5 = (-4) \cdot 16^2 \equiv (-4) \cdot 3^2 = (-4) \cdot 9 \equiv (-4)^2 = 16 \equiv 3 \pmod{13} .$$

Thus the remainder is 3.

Note: The solution can be simplified by observing that $3^3 \equiv 1 \pmod{13}$.

b) Note that $99 \equiv 7 \pmod{23}$, so $99^{999999} \equiv 7^{999999} \pmod{23}$. By Euler's theorem, $7^{22} \equiv 1 \pmod{23}$. Now we want to find r such that $999999 = 22 \cdot k + r$ and $0 \leq r < 22$. Note that both 999999 and 22 are divisible by 11 and therefore so is r. Thus $r = 0$ or $r = 11$. Since r must be odd, we have $r = 11$ (alternatively, you can find r by performing division algorithm). It follows that

$$7^{999999} \equiv 7^{11} = 7 \cdot 49^5 \equiv 7 \cdot 3^5 = 21 \cdot 81 \equiv (-2) \cdot 12 = -24 \equiv 22 \pmod{23} .$$

Thus the remainder is 22.

c) Note that $29 \equiv 9 = 3^2 \pmod{20}$, so $29^{198} \equiv 3^{396} \pmod{20}$. Now $\phi(20) = \phi(4 \cdot 5) = \phi(4)\phi(5) = 2 \cdot 4 = 8$, so $3^8 \equiv 1 \pmod{20}$. Now $396 = 8 \cdot 49 + 4$. Thus

$$3^{396} \equiv 3^4 = 81 \equiv 1 \pmod{20} .$$

Thus the remainder is 1.

d) Note that $\phi(14) = \phi(2 \cdot 7) = \phi(2)\phi(7) = 6$. Also, $1000000 = 6k + 4$ for some k. Thus

$$3^{1000000} \equiv 3^4 = 81 \equiv 11 \pmod{14} .$$

Thus the remainder is 11.

Problem 13. Prove that if n is relatively prime to 72 then $n^{12} \equiv 1 \pmod{72}$.

Solution: Note that $72 = 8 \cdot 9$. Since $\phi(8) = 4$, we have $n^4 \equiv 1 \pmod 8$ for any n relatively prime to 8. It follows that $n^{12} \equiv 1 \pmod 8$ for any n such that $\gcd(8, n) = 1$.

Similarly, $\phi(9) = 6$ so $n^6 \equiv 1 \pmod 9$ for any n relatively prime to 9. It follows that if $\gcd(n, 9) = 1$ then $n^{12} \equiv 1 \pmod 9$.

Suppose that $\gcd(n, 72) = 1$. Then both $\gcd(n, 8) = 1 = \gcd(n, 9)$. Thus $n^{12} \equiv 1 \pmod 8$ and $n^{12} \equiv 1 \pmod 9$. In other words, $8|n^{12} - 1$ and $9|n^{12} - 1$. Since 8 and 9 are relatively prime, we have $8 \cdot 9 = 72|n^{12} - 1$, i.e. $n^{12} \equiv 1 \pmod{72}$.

Remark. Note that what we proved is stronger than what Euler's theorem implies for 72. In fact, $\phi(72) = \phi(8)\phi(9) = 4 \cdot 6 = 24$, so we only get $n^{24} \equiv 1 \pmod{72}$ from Euler's theorem for 72.

Problem 14. Let p, q be distinct prime numbers. Prove that

$$p^{q-1} + q^{p-1} \equiv 1 \pmod{pq} .$$

Solution: Since $p \neq q$ are prime numbers, we have $\gcd(p, q) = 1$. By Fermat's Little Theorem, $p^{q-1} \equiv 1 \pmod q$. Clearly $q^{p-1} \equiv 0 \pmod q$. Thus

$$p^{q-1} + q^{p-1} \equiv 1 \pmod q .$$

Exchanging the roles of p and q in the above argument, we prove that

$$p^{q-1} + q^{p-1} \equiv 1 \pmod p .$$

In other words, $p^{q-1} + q^{p-1} - 1$ is divisible by both p and q. Since p and q are relatively prime, we conclude that $p^{q-1} + q^{p-1} - 1$ is divisible by pq, i.e. $p^{q-1} + q^{p-1} \equiv 1 \pmod{pq}$.

Problem 15. Let m, n be positive integers such that $m|n$. Prove that $\phi(m)|\phi(n)$ and that $\phi(mn) = m\phi(n)$

Solution: Since $m|n$, we can number the prime divisors of n such that

$$m = p_1^{a_1}...p_s^{a_s} \text{ and } n = p_1^{b_1}...p_s^{b_s}p_{s+1}^{b_{s+1}}...p_t^{b_t},$$

where $t \geq s$, $0 < a_i \leq b_i$ for $i = 1, 2, ..., s$ and $0 < b_i$ for $i > s$, and $p_1, ..., p_t$ are pairwise distinct prime numbers.

Now

$$\phi(m) = (p_1 - 1)p_1^{a_1-1}...(p_s - 1)p_s^{a_s-1}$$

and

$$\phi(n) = (p_1 - 1)p_1^{b_1-1}...(p_s - 1)p_s^{b_s-1}(p_{s+1} - 1)p^{b_{s+1}-1}...(p_t - 1)p_t^{b_t-1}.$$

It is clear now that $\phi(m)|\phi(n)$. Moreover, $mn = p_1^{a_1+b_1}...p_s^{a_s+b_s}p_{s+1}^{b_{s+1}}...p_t^{b_t}$ and

$$\phi(mn) = (p_1 - 1)p_1^{a_1+b_1-1}...(p_s - 1)p_s^{a_s+b_s-1}(p_{s+1} - 1)p^{b_{s+1}-1}...(p_t - 1)p_t^{b_t-1} = m\phi(n).$$

Second solution: Suppose that the result is false and let $m|n$ be a counterexample with smallest possible n. Clerly $m > 1$ (since the result holds trivially for $m = 1$). Let p be a prime divisor of m. Thus we can write $m = p^a m_1$ and $n = p^b n_1$ for some $0 < a \leq b$

and natural numbers n_1, m_1 not divisible by p. Since $m_1|n = p^b n_1$ and $\gcd(p, m_1) = 1$, we have $m_1|n_1$. Also

$$\phi(m) = \phi(p^a)\phi(m_1) = (p-1)p^{a-1}\phi(m_1),$$
$$\phi(n) = \phi(p^b)\phi(n_1) = (p-1)p^{b-1}\phi(n_1)$$

and

$$\phi(mn) = \phi(p^{a+b})\phi(m_1 n_1) = (p-1)p^{a+b-1}\phi(m_1 n_1).$$

Since $m_1|n_1$ and $n_1 < n$, the result is true for m_1, n_1, i.e. $\phi(m_1)|\phi(n_1)$ and $\phi(m_1 n_1) = m_1\phi(n_1)$. But then

$$\phi(m) = (p-1)p^{a-1}\phi(m_1)|(p-1)p^{b-1}\phi(m_1)|(p-1)p^{b-1}\phi(n_1) = \phi(n)$$

and

$$\phi(mn) = (p-1)p^{a+b-1}\phi(m_1 n_1) = p^a m_1 (p-1)p^b\phi(n_1) = m\phi(n)$$

so the result is true for m, n contrary to our assumption. The contradiction proves that no counterexample to our result exists.

Problem 16. Compute $\phi(2592)$, $\phi(111111)$, $\phi(15!)$.

Solution: We have

$$2592 = 4 \cdot 648 = 4 \cdot 4 \cdot 162 = 2^5 \cdot 81 = 2^5 \cdot 3^4$$

Thus $\phi(2592) = \phi(2^5)\phi(3^4) = 2^4 \cdot 2 \cdot 3^3 = 2^5 \cdot 3^3$.

Clearly 111111 is divisible by 11,3 so

$$111111 = 11 \cdot 10101 = 11 \cdot 3 \cdot 3367$$

Now 3367 is divisible by 7: $3367 = 7 \cdot 481$. The next prime to consider is 13 and indeed $481 = 13 \cdot 37$. Thus $111111 = 3 \cdot 7 \cdot 11 \cdot 13 \cdot 37$ and

$$\phi(111111) = \phi(3)\phi(7)\phi(11)\phi(13)\phi(37) = 2 \cdot 6 \cdot 10 \cdot 12 \cdot 36 = 2^7 \cdot 3^4 \cdot 5.$$

Finally $15! = 2^{11} \cdot 3^6 \cdot 5^3 \cdot 7^2 \cdot 11 \cdot 13$, so

$$\phi(15!) = \phi(2^{11})\phi(3^6)\phi(5^3)\phi(7^2)\phi(11)\phi(13) = 2^{10} \cdot 2 \cdot 3^5 \cdot 4 \cdot 5^2 \cdot 6 \cdot 7 \cdot 10 \cdot 12 = 2^{17} \cdot 3^7 \cdot 5^3 \cdot 7.$$

Problem 17. Prove that 561 is a composite number and $a^{561} \equiv a \pmod{561}$ for every integer a.

Solution: Let us first note the following corollary from Fermat's Little Theorem:

Proposition 1. *Let p be a prime number. For any integer n and any natural number k we have $n^{k(p-1)+1} \equiv n \pmod{p}$.*

Indeed, if $p|a$ then both sides of the congruence are $\equiv 0 \pmod{p}$ and if $\gcd(p, a) = 1$ then $n^{p-1} \equiv 1 \pmod{p}$ and $n^{k(p-1)+1} = n(n^{p-1})^k \equiv n \pmod{p}$.

We have $561 = 3 \cdot 187 = 3 \cdot 11 \cdot 17$, so 561 is not a prime. Now $561 = 280 \cdot 2 + 1 = 56 \cdot 10 + 1 = 35 \cdot 16 + 1$. By the proposition, $n^{561} \equiv n \pmod{3}$, $n^{561} \equiv n \pmod{11}$ and $n^{561} \equiv n \pmod{17}$ for every integer n. Thus $n^{561} - n$ is divisible by 3, 11, 17 and since these numbers are pairwise relatively prime, $3 \cdot 11 \cdot 17|n^{561} - n$, i.e. $n^{561} \equiv n \pmod{561}$ for every integer n.

Problem 18. Let p be a prime number and let n be a positive integer such that $p^4|n^3$. Prove that $p^2|n$.

Solution: Suppose that $p^k \parallel n$ (i.e. p^k is the highest power of p which divides n). Then $p^{3k} \parallel n^3$ and therefore $3k \geq 4$. Since k is an integer, we have $k \geq 2$ and therefore $p^2|n$.

Second solution: Clearly $p^4|n^3$ implies that $p|n^3$. Since p is prime we have $p|n$, i.e. $n = pm$ for some integer m. Now $p^4|n^3 = p^3m^3$ implies that $p|m^3$. Again, since p is a prime number, we get $p|m$. It follows that $m = pk$ for some integer k, so $n = pm = p^2k$, i.e. $p^2|n$.