(1) Let p_1, p_2 be distinct prime numbers.

Using the method from class give a careful proof of the formula

$$\phi(p_1^{k_1} p_2^{k_2}) = (p_1^{k_1} - p_1^{k_1-1})(p_2^{k_2} - p_2^{k_2-1})$$

Solution

Let $n = p_1^{k_1} p_2^{k_2}$ The only prime divisors of n are p_1 and p_2 so if $gcd(m,n) \neq 1$ then either $p_1|m$ or $p_2|m$. Thus to compute $\phi(n)$ we need to write down the numbers $1, 2, \ldots n$, cross out those that are divisible by p_1 or p_2 and count how many are left.

First let us cross out the numbers divisible by p_1. They are $1 \cdot p_1, 2 \cdot p_1, \ldots, (\frac{n}{p_1})p_1$. Thus there are $\frac{n}{p_1} = p_1^{k_1-1} p_2^{k_2}$ of them.

Next, we cross out the numbers divisible by p_2. They are $1 \cdot p_2, 2 \cdot p_2, \ldots, (\frac{n}{p_2})p_2$. Thus there are $\frac{n}{p_2} = p_1^{k_1} p_2^{k_2-1}$ of them.

Note however, that we crossed out twice the numbers which are divisible by both p_1 and p_2, i.e. the numbers divisible by $p_1 p_2$. They are $1 \cdot p_1 p_2, 2 \cdot p_1 p_2, \ldots, (\frac{n}{p_1 p_2})p_1 p_2$. There are $\frac{n}{p_1 p_2} = p_1^{k_1-1} p_2^{k_2-1}$ of them.

Thus, $\phi(n) = p_1^{k_1} p_2^{k_2} - p_1^{k_1-1} p_2^{k_2} - p_1^{k_1} p_2^{k_2-1} + p_1^{k_1-1} p_2^{k_2-1} = (p_1^{k_1} - p_1^{k_1-1})(p_2^{k_2} - p_2^{k_2-1})$.

(2) Let a, b, c be natural numbers. Let (a, b, c) be the largest natural number that divides a, b and c.

(a) Prove that $gcd(a, b, c) = gcd(gcd(a, b), c)$.

(b) Prove that the equation $ax + by + cz = gcd(a, b, c)$ has an integer solution.

Solution

(a) Let $d = gcd(a, b, c)$ and let $d_1 = gcd(gcd(a, b), c)$. Then $d|a, d|b$ and $d|c$. Therefore, $d|gcd(a, b)$ and $d|c$ and therefore $d|d_1 = gcd(gcd(a, b), c)$. Conversely, $d_1|gcd(a, b)$ and $d_1|c$ and hence $d_1|a, d_1|b, d_1|c$. Therefore $d_1|gcd(a, b, c) = d$.
This means that $d|d_1$ and $d_1|d$ and hence $d = d_1$. $\square$.

(b) It was proved in class that for any integer a, b the equation $ax + by = gcd(a, b)$ admits an integer solution x_0, y_0. Therefore, the equation $k \cdot gcd(a, b) + lc = gcd(gcd(a, b), c)$ also admits an integer solution k_0, l_0. But by part a) $gcd(a, b, c) = gcd(gcd(a, b), c)$. Therefore $k_0 \cdot gcd(a, b) + l_0 c = gcd(a, b, c)$. Substituting $gcd(a, b) = ax_0 + by_0$ we get $gcd(a, b, c) = k_0 \cdot gcd(a, b) + l_0 c = k_0 \cdot (ax_0 + by_0) + l_0 c = k_0 x_0 a + k_0 y_0 b + l_0 c$. $\square$.

(3) Find $22^{201} (\mod 30)$.

Note: Note that $gcd(22, 30) \neq 1$!

Solution

Since $gcd(22, 30) \neq 1$ we can not use Euler's theorem directly. Let us therefore first find $22^{201} (\mod 15)$. Since $gcd(22, 15) = 1$, by Euler's theorem we have $22^{\phi(15)} \equiv 1 \pmod{15}$. We have $\phi(15) = \phi(3 \cdot 5) =$

$(3-1)\cdot(5-1) = 8$. Thus, $22^8 \equiv 1 \pmod{15}$. Therefore, $22^{201} \equiv 22^{200}\cdot 22 \equiv (22^8)^{25}\cdot 22 \equiv 1\cdot 22 \equiv 7 \pmod{15}$.

Thus, $15|22^{201}-7$. However, $2 \nmid 22^{201}-7$ and therefore $30 \nmid 22^{201}-7$. To fix this observe that $7 \equiv 7+15 = 22 \pmod{15}$ and thus $22^{201} \equiv 22 \pmod{15}$,i.e. $15|22^{201}-22$. But now we also have that $2|22^{201}-22$ and hence $30|22^{201}-22$, i.e. $22^{201} \equiv 22 \pmod{30}$.

Answer: $22^{201} \equiv 22 \pmod{30}$.

(4) Find $6^{3^{101}} \pmod{22}$.

Solution

Let us first find $6^{3^{101}} \pmod{11}$. We have that $gcd(6,11) = 1$ and hence $6^{\phi(11)} = 6^{10} \equiv 1 \pmod{11}$. Thus to find $6^{3^{101}} \pmod{11}$ we first need to find $3^{101} \pmod{10}$. because if $3^{101} = 10k+r$ for some k and $r < 10$ then $6^{3^{101}} = 6^{10k+r} = (6^{10})^k\cdot 6^r \equiv 6^r \pmod{11}$ which is computable because $r < 10$.

To find $3^{101} \pmod{10}$ we notice that $gcd(3,10) = 1$ and hence $3^{\phi(10)} = 3^4 \equiv 1 \pmod{10}$. this can also be checked directly because $3^4 = 81$. Therefore, $3^{101} = (3^4)^{25}\cdot 3 \equiv 1\cdot 3 \equiv 3 \pmod{10}$ or $3^{101} = 10k+3$ for some integer k.

Therefore, $6^{3^{101}} = 6^{10k+3} = (6^{10})^k\cdot 6^3 \equiv 6^3 \pmod{11} \equiv 7 \pmod{11}$. This means that $11|6^{3^{101}}-7$. Since 7 is odd $2 \nmid 6^{3^{101}}-7$. But by the same argument as in the previous problem, observe that $6^{3^{101}} \equiv 7 \equiv 18 \pmod{11}$ and hence $11|6^{3^{101}}-18$. Since we also have that $2|6^{3^{101}}-18$ this implies that $22|6^{3^{101}}-18$, i.e. $6^{3^{101}} \equiv 18 \pmod{22}$.

Answer: $6^{3^{101}} \equiv 18 \pmod{22}$.

(5) Solve the following congruence equations
 (a) $6x \equiv 9 \pmod{33}$
 (b) $24x \equiv 7 \pmod{35}$

Solution

a) $6x \equiv 9 \pmod{33}$ is equivalent to $33|6x-9$ or $33k = 6x-9$ for some integer k. Dividing this equation by 3 we get an equivalent equation $11k = 2x-3$ or $2x \equiv 3 \pmod{11}$. Thus $6x \equiv 9 \pmod{33}$ is equivalent to $2x \equiv 3 \pmod{11}$. Observe that $x \equiv 7 \pmod{11}$ works since $2\cdot 7 = 14 \equiv 3 \pmod{11}$.

Since $gcd(2,11) = 1$ this is the only solution mod 11.

Answer: $x \equiv 7 \pmod{11}$.

From textbook:

(6) # 21 on page 59: Let p be an odd prime and let $m = 2p$ We need to prove that $a^{m-1} \equiv a \pmod{m}$ for any natural a. Let us first show that $a^{m-1} \equiv a \pmod{p}$. If $p|a$ then $a^{m-1} \equiv 0 \equiv a \pmod{p}$. If $p \nmid a$ then $a^{p-1} \equiv 1 \pmod{p}$ by Fermat's theorem and hence $a^{2(p-1)} = a^{2p-2} \equiv 1 \pmod{p}$ also. Multiplying this by a we get $a^{2p-1} \equiv 1 \pmod{p}$. Thus in either case $a^{m-1} \equiv a \pmod{p}$.

But it is also easy to see that $a^{m-1} \equiv a \pmod 2$: If a is even then both a^{m-1} and a are even and if a is odd then both a^{m-1} and a are odd.

Thus $2|a^{m-1} - a$ and $p|a^{m-1} - a$ and hence $2p|a^{m-1} - a$ since p is a prime different from 2. $\square$.

(7) #1 on page 45: We have $p = 5, q = 7, E = 7, R = 17$. To verify that $D = 5$ is a decryptor we ned to check that $DE \equiv 1 \pmod \phi)(N)$ where $N = pq = 35$. we compute $\phi(35) = \phi(5 \cdot 7) = 4 \cdot 6 = 24$. Since $5 \cdot 5 = 25 \equiv 1 \pmod{24}$ we see that $D = 5$ is a decryptor.

To find the original message M we need to compute $R^D \pmod N$. In our case this is $17^5 \pmod{35}$. We have $17^2 = 289 = 280 + 9 = 35 \cdot 8 + 9$ and hence $17^2 \equiv 9 \pmod{35}$. Therefore, $17^4 \equiv 9^2 \equiv 81 \equiv 11 \pmod{35}$. Therefore, $M \equiv 17^5 \equiv 17^4 \cdot 17 \equiv 11 \cdot 17 \equiv 187 \equiv 12 \pmod{35}$.

Answer: $M = 12$.

(8) #2 on page 45: We have $N = 21, E = 5$.

(a) To encrypt $M = 7$ we have to compute $R = M^E \pmod N$ or $7^5 \pmod{21}$. We have $7^2 = 49 = 42 + 7 \equiv 7 \pmod{21}$. This easily implies by induction that $7^k \equiv 7 \pmod{21}$ for any $k \geqslant 1$. In particular, $7^5 \equiv 7 \pmod{21}$.

(b) To check that $D = 5$ is a decryptor we need to verify that $DE \equiv 1 \pmod{\phi(N)}$. We have $\phi(21) = \phi(3 \cdot 7) = 2 \cdot 6 = 12$. We compute $5 \cdot 5 = 25 \equiv 1 \pmod{12}$ which means that $D = 5$ is a decryptor.

(c) To decrypt the original message we have to compute $R^D \pmod N$ which in ours case is $7^5 \pmod{21} \equiv 7 \pmod{21}$. This is the original number $M = 7$.