MATH 430 Midterm II

Qilin Ye

October 20, 2020

Problem 1

Show that $\varphi(n)$ is even for all integer $n \geqslant 3$.

Solution

If $n \geqslant 3$, then we know $n-1 \not\equiv 1 \pmod{n}$. On the other hand, in $(\mathbb{Z}/n\mathbb{Z})^*$, $o(n-1) = 2$ since $(n-1)^2 = (-1)^2 = 1$. Clearly $n-1 \in (\mathbb{Z}/n\mathbb{Z})^*$. By Lagrange's theorem we immediately know $o(n-1)$ divides $|(\mathbb{Z}/n\mathbb{Z})^*|$, i.e., $|(\mathbb{Z}/n\mathbb{Z})^*|$ is even. But this is exactly $\varphi(n)$. Therefore $\varphi(n)$ is even. □

Problem 2

Show that $a^{560} \equiv 1 \pmod{561}$ for all integers a with $\gcd(a, 561) = 1$.

Solution

First, let us prime factorize 561 as $3 \cdot 11 \cdot 17$. We know that if $\gcd(a, 561) = 1$ then $\gcd(a, 3) = \gcd(a, 11) = \gcd(a, 17) = 1$, for if $\gcd(a, 3) = x > 1$ then $x \mid 3, x \mid a$, and $x \mid 561$; then $x \mid \gcd(x, 561)$ and $\gcd(x, 561) = 1$ cannot hold (likewise for the other two cases). Now we apply Fermat's little theorem thrice.

(1) Since $\gcd(x, 3) = 1$, we know $x \in (\mathbb{Z}/3\mathbb{Z})^*$ and $x^2 \equiv 1 \pmod{3}$. Therefore
$$x^{560} = (x^2)^{280} = 1^{280} \equiv 1 \pmod{3}.$$

(2) Since $\gcd(x, 11) = 1$, we know $x \in (\mathbb{Z}/11\mathbb{Z})^*$ and $x^{10} \equiv 1 \pmod{11}$. Therefore
$$x^{560} = (x^{10})^{56} = 1^{56} \equiv 1 \pmod{11}.$$

(3) Since $\gcd(x, 17) = 1$, we know $x \in (\mathbb{Z}/17\mathbb{Z})^*$ and $x^{16} \equiv 1 \pmod{17}$. Therefore $x^{560} = (x^{16})^{35} = 1^{35} \equiv 1 \pmod{17}$.

To sum up, we've just shown that if $\gcd(x, 561) = 1$ then

$$x^{560} \begin{cases} \equiv 1 \pmod{3} \\ \equiv 1 \pmod{11} \\ \equiv 1 \pmod{17} \end{cases}$$

By inspection we see that $x^{560} \equiv 1 \pmod{3 \cdot 11 \cdot 17}$ is a solution, i.e., x^{560} can be of form $561k + 1$. Since $\operatorname{lcm}(3, 11, 17) = 561$, this is the only solution. Otherwise we would have the absurd contradiction that $561 \mid n-1$ for some $0 \leqslant x \leqslant 560$ different than 1 as both n and 1 satisfy the three congruence relations. Therefore $x^{560} \equiv 1 \pmod{561}$. □

Problem 3

Show that there are infinitely many primes which are 5 mod 6 without using Dirichlet's Theorem.

Solution

First notice that primes besides 2 and 3 can only be of form $6k + 1$ or $6k + 5$ since $6k + 2$ and $6k + 4$ are multiples of 2 and $6k + 3$ divides 3. Suppose, by contradiction, that there were only finitely many primes 5 mod 6. Then we can list them as $p_1, p_2, \ldots, p_n$. Now take the product and define

$$N := 6(p_1 p_2 \ldots p_n) - 1.$$

Clearly $N \equiv 5 \pmod{6}$ (and it's odd). In addition, since all p's divide $N + 1$ we know they don't divide N. Now we want to show that N is yet another prime of form $6k + 5$. Suppose not, then it must be the product of some prime factors. Since $2 \nmid 6$ it is not an option. 3 is not an option, either. We know the p's are also not possible. Therefore we are left with primes of form $6k + 1$. However, the product of these primes will *always* have remainder 1 when divided by 6 and they can never get N which is 5 mod 6. Hence we've derived a contradiction, and there cannot be finitely many primes 5 mod 6 at the first place.

Remark

We could also define $N := (2p_1p_2 \dots p_n)^2 + 1$. Then $N \equiv 4(-1)^{2n} + 1 \equiv 5 \pmod 6$. Then the same argument follows.

Problem 4

Let $n \geqslant 3$ be an integer and let $A_n = \{a \mid 1 \leqslant a \leqslant n-1, \gcd(a,n) = 1\}$. Let b be the product of all elements $a \in A_n$. Show that $b \equiv 1 \pmod n$ or $b \equiv -1 \pmod n$.

Solution

We know that if $\gcd(a,n) = 1$ then $a \in (\mathbb{Z}/n\mathbb{Z})^*$, and A_n can be treated as $(\mathbb{Z}/n\mathbb{Z})^*$. Notice that *each* element in $(\mathbb{Z}/n\mathbb{Z})^*$ has an inverse, but there are two possibilities: $a = a^{-1}$ or $a \neq a^{-1}$. Let us define

$$A_{n_1} := \{a \in (\mathbb{Z}/n\mathbb{Z})^* \mid a = a^{-1}\} \text{ and } A_{n_2} := \{a \in (\mathbb{Z}/n\mathbb{Z})^* \mid a \neq a^{-1}\}.$$

Clearly $A_{n_1} \cap A_{n_2} = \varnothing$ and $A_{n_1} \cup A_{n_2} = A_n$. If $x \in A_{n_2}$ it follows that $x \neq x^{-1} \implies (x^{-1})^{-1} \neq x^{-1}$ so $x^{-1} \in A_{n_2}$ as well. In other words, elements in A_{n_2}, should there be any, are "paired", and the product within each pair is $xx^{-1} = 1$. Therefore the product of all elements in A_{n_2} is $1 \cdot 1 \cdots = 1$.

On the other hand, let's look at A_{n_1}. Notice that if $y \in A_{n_1}$, then so is $n-y$ since if $y^2 = 1 = (-y)^2 = (n-y)^2$. Therefore elements in A_{n_1} are also paired. Their product, however, is $y(n-y) = yn - y^2 = -1$. Therefore the products of all elements of A_{n_1} is $(-1)^k = \pm 1$ depending on how many pairs there are. Since $A_{n_1} \cup A_{n_2} = A_n$ we know that

$$b = \prod a : a \in A_n = \left[\prod a_1 : a_1 \in A_{n_1}\right] \cdot \left[\prod a_2 : a_2 \in A_{n_2}\right] = 1 \cdot \pm 1 = \pm 1.$$

(A quick check suggests that if $n = 8$ then $b = 1 \cdot 3 \cdot 5 \cdot 7 = 1$ while $n = 6$ suggests $b = 1 \cdot 5 = -1$. Hence 1 and -1 are both possible.)

Problem 5

Let $n \geqslant 3$ be an integer and let $A_n := \{a \mid 1 \leqslant a \leqslant n-1, \gcd(a,n) = 1\}$. Assume further that there is an element $g \in A_n$ that generates this group. Its order is therefore $\varphi(n)$. Let b be the product of all elements $a \in A_n$. Show $b \equiv -1 \pmod n$.

Solution

Continuing from last problem: now suppose g is a generator. If $x^2 = 1$ then either $x = 1$ or $o(x) = 2$. If it is the latter case, suppose $x = g^k$ for some $1 \leqslant k < \varphi(n)$ [since $g^{\varphi(n)}$ is taken by 1 and is no longer available]. Then, on one hand we have $g^{\varphi(n)} = 1$ and on the other hand, $x^2 = 1$. Thus

$$(g^k)^2 = g^{2k} = 1 = g^{\varphi(n)} \implies g^{\varphi(n)-2k} = 1.$$

This means $\varphi(n) \mid \varphi(n) - 2k$. Since $1 \leqslant k < \varphi(n)$, we have $-\varphi(n) < \varphi(n) - 2k < \varphi(n)$, and so the only possibility is if $k = \varphi(n)/2$. Note that from the result of problem (1) we know k is guaranteed to be an integer. On the other hand we see that $n - 1 \neq 1$ and $(n-1)^2 = 1$. Therefore $n - 1$ is precisely $g^{\varphi(n)/2}$ and it is the *only* other element in A_{n_1} besides 1 the identity.

We've shown that $A_{n_1} = \{1, n-1\}$, and the product of all elements in this set is $1(n-1) = -1$. Everything else goes into A_{n_2}, where they again form "pairs" of product 1. Again, similar to the previous problem, we have $b = -1 \cdot (1 \cdot 1 \ldots) = -1$. □