math115A hw6

Jonas Chen

October 10, 1000

Problem 1

> Find the orders of the integers 2,3, and 5
> (a) modulo 17
> (b) modulo 19
> (c) modulo 23

Solution

Firstly, the 2, 3, and 5 are each coprime respectively to 17,19, and 23 so the definition of order can be used.

From class we know that the order of $a \bmod n$ must divide $\phi(n)$

Here, $\phi(17) = 16, \phi(19) = 18, \phi(23) = 22$. Therefore the order is at most $\phi(n)$ or if the order is less, it must divide $\phi(n)$. Checking if the divisors d_i of 16, 19, 23 are the smallest numbers satisfying $a^{d_i} \equiv 1 (\bmod n)$ in increasing order gives us the following for parts (a),(b),(c) respectively:

(a) $2^2 \equiv 4 (\bmod 17)$

$2^4 \equiv 16 (\bmod 17)$

$2^8 = 256 \equiv 1 (\bmod 17)$ therefore the order of 2 mod 17 is 8

Similarly the orders of 3 and 5 (mod 17) are 16 and 16 respectively

(b)

Similar to (a) we have that $2, 3, 5$ have orders $18, 18, 9$ mod 19 respectively

(c)

Similar to (a) and (b) we have that $2, 3, 5$ have orders $11, 11, 22$ mod 23 respectively

Problem 2

> Establish each of the following statements below:
> (a) if a has order hk modulo n, then a^h has order k modulo n
> (b) if a has order $2k$ modulo an odd prime p , then $a^k \equiv -1 \bmod p$

Solution

(a) Suppose that a has order hk modulo n

Then it follows that $a^{hk} \equiv 1 (\bmod n)$ and it follows that $\left(a^h\right)^k \equiv 1 (\bmod n)$ so that k is a possible candidate for the order of a^h

We can show that a^h has order at most k since if there exists $1 \leq z < k$ such that $\left(a^h\right)^z \equiv 1 (\bmod n)$ then it follows that $a^{hz} \equiv 1 (\bmod n)$, but since hk is the order of a we have that $hk < hz \Rightarrow k < z$ which is a contradiction. Therefore k is the smallest possible number such that $\left(a^h\right)^k \equiv 1 (\bmod n)$

(b)

Suppose that a has order $2k$ then $a^{2k} \equiv 1 (\bmod p)$ implies that $a^{2k} - 1 \equiv 0 (\bmod p)$ therefore $p \mid a^{2k} - 1 = \left(a^k + 1\right)\left(a^k - 1\right)$ which means that either or $a^k \equiv 1 (\bmod p)$ or that $a^k \equiv -1 (\bmod p)$

But $a^k \equiv 1 (\bmod p)$ cannot hold since $2k$ is the order of $a (\bmod p)$

Therefore the other case, that $a^k \equiv -1 (\bmod p)$ holds

Problem 3

> Prove that $\phi(2^n - 1)$ is a multiple of n for any $n \geq 1$. [Hint: The integer 2 has order n modulo $2^n - 1$]

Solution

From the hint we know that $2^n \equiv 1 (\operatorname{mod} 2^n - 1)$ This equivalence holds since $2^n - 1 \equiv 0 (\operatorname{mod} 2^n - 1)$ holds.

Note that if n is the order of $2 \operatorname{mod} 2^n - 1$ then $n \mid \phi(2n - 1) \Rightarrow \phi(2^n - 1) = nk$ for some $k \geq 1$ i.e. $\phi(2^n - 1)$ is a multiple of n as desired.

To show that n is the order of $2 \operatorname{mod} 2^n - 1$ we can first suppose that there exists $1 \leq z < n$ such that $2^z \equiv 1 (\operatorname{mod} 2^n - 1)$

This implies that $2^n - 1 \mid 2^z - 1$ but since $2^n - 1 > 2^z - 1$ this cannot be true. Therefore z cannot exist and n is the order of $2 \operatorname{mod} 2^n - 1$

Problem 4

> Prove the following assertions:
> (a) The odd prime divisors of the integer $n^2 + 1$ are of the form $4k + 1$. [Hint: if p is an odd prime, then $n^2 \equiv -1 \bmod p$ implies that $4 \mid \phi(p)$]
> (b) The odd prime divisors of the integer $n^4 + 1$ are of the form $8k + 1$

Solution

(a) If p is an odd prime divisor of $n^2 + 1$, then $n^2 + 1 \equiv 0 (\operatorname{mod} p) \Rightarrow n^2 \equiv -1 (\operatorname{mod} p) \Rightarrow n^4 \equiv 1 (\operatorname{mod} p)$

Next, we can show that p is coprime to n

Suppose p is not coprime to n, then $n = kp$ for some k (since p must be a factor of n)

Since p is a divisor of $n^2 + 1$ we expect that $(kp)^2 + 1 \equiv 0 (\operatorname{mod} p)$ holds, but this is not true since $p \mid k^2 p^2$ but $p \nmid 1$, which show that p is not a divisor of $n^2 + 1$ which is a contradiction. therefore p is coprime to n

We can then apply Euler's theorem to obtain $n^{\phi(p)} \equiv 1 (\operatorname{mod} p) \Leftrightarrow n^{p-1} \equiv 1 (\operatorname{mod} p)$

From the first line we have $1 \equiv n^4 \equiv n^{p-1} (\operatorname{mod} p)$ which implies that $4 \mid p - 1 = \phi(p)$ since $n^{4k} = \left(n^4\right)^k \equiv \left(n^{p-1}\right)^k \equiv \left(n^{p-1}\right) (\operatorname{mod} p)$ and therefore $p - 1 = 4k \Rightarrow p = 4k + 1$

(b)

Similar to part (a) we can argue that if p is an odd prime divisor of $n^4 + 1$ then $n^8 \equiv 1 (\operatorname{mod} p)$

Similarly, n and p are coprime and using Euler's theorem we have $n^{p-1} \equiv 1 (\operatorname{mod} p)$

Therefore $1 \equiv n^8 \equiv n^{p-1} (\operatorname{mod} p)$ implies that $8 \mid p - 1 \Leftrightarrow 8k = p - 1 \Leftrightarrow p = 8k + 1$

Problem 5

> Let r be the primitive root modulo p, where p is an odd prime. Prove the following:
>
> (a) The congruence $r^{(p-1)/2} \equiv -1 (\operatorname{mod} p)$ holds.
> (b) If r' is any other primitive root modulo p, then rr' is not a primitive root modulo p. [Hint: From part (a), $(rr')^{(p-1)/2} \equiv 1 (\operatorname{mod} p)$]
> (c) If the integer r' is such that $rr' \equiv 1 (\operatorname{mod} p)$, then r' is also a primitive root modulo p

Solution

(a) The problem statement implies that $r^{p-1} \equiv 1 (\operatorname{mod} p)$ implies that

$$p \mid r^{p-1} - 1 = \left(\left(r^{(p-1)/2}\right) - 1\right)\left(\left(r^{(p-1)/2}\right) + 1\right)$$

However $p \nmid \left(\left(r^{(p-1)/2}\right) - 1\right)$ since r has primitive root $p-1$, and therefore $\left(r^{(p-1)/2}\right) \not\equiv 1 (\operatorname{mod} p)$

Therefore it must be true that $p \mid \left(r^{p-1/2}\right) + 1$ which implies that $r^{p-1/2} \equiv -1 (\operatorname{mod} p)$

(b) The statement from the hint holds since $(rr')^{p-1/2} = (r)^{p-1/2}(r')^{p-1/2} \equiv (-1)(-1) = 1 (\operatorname{mod} p)$ using the result from part (a), since rr' must have an order less than or equal to $(p-1)/2$ then it cannot have order $\phi(p) = p-1$ and therefore rr' is not a primitive root modulo p

(c)

We would like to show that r' has order $\phi(p) = p-1$ i.e. $p-1$ is the smallest integer such that $(r')^{p-1} \equiv 1 (\operatorname{mod} p)$

Then if we consider some $1 \leq z < p-1$ and call z the order of r' then

$$rr' \equiv 1 (\operatorname{mod} p) \Leftrightarrow (rr')^z \equiv 1^z (\operatorname{mod} p) \Leftrightarrow r^z r'^z \equiv 1 (\operatorname{mod} p) \Leftrightarrow r^z \equiv 1 (\operatorname{mod} p)$$

but since r is a primitive root modulo p it must have order $p-1$ and therefore z canonot satisfy the equation $r^z \equiv 1 (\operatorname{mod} p)$, which contradict $rr' \equiv 1 (\operatorname{mod} p)$ therefore $p-1$ is the order of $r' (\operatorname{mod} p)$

Note that r' is not divisible by p since if it were then $rr' \equiv 1 (\operatorname{mod} p)$ cannot hold, and therefore we can use Fermat's little theorem to assert that $(r')^{p-1} \equiv 1 (\operatorname{mod} p)$ holds.

Problem 6

> For any prime $p > 3$, prove that the primitive roots modulo p occur in incongruent pairs r, r', where $rr' \equiv 1 \pmod p$. [Hint: If r is a primitive root modulo p, consider the integer $r' = r^{p-2}$]

Solution

We can first try to show that if r is a primitive root modulo p then $r' = r^{p-2}$ is also a primitive root modulo p

We can observe that $rr' = r \cdot r^{p-2} = r^{p-1} \equiv 1 \pmod p$ Therefore r' is a primitive root given r is also a primitive root

Claim: $r \not\equiv r^{p-2} \pmod p$ This claim holds for $p = 3$ but does not hold for any $p > 3$

Suppose the r, r' are congruent than for any $p > 3$ we have that

$$r \equiv r^{p-2} \pmod p \text{ if and only if } r - r^{p-2} \equiv 0 \pmod p$$

where $p - 2 > 2$

This implies that p must divide $r(1 - r^{p-3})$ which is not possible since $(p, r) = 1$ by the definition of order. In addition, p cannot divide $1 - r^{p-3}$ since this quantity is less than 1, and $p > 2 \forall p$

Therefore r, r' are incongruent

Problem 7

> Suppose that p is a prime. Use the fact that there exists a primitive root modulo p to give a different proof of Wilson's theorem. [Hint: show that if r is a primitive root modulo p , then $(p-1)! \equiv r^{1+2+\ldots+(p-1)} \pmod{p}$]

Solution

The hint follows from a result in shown in class which shows that the numbers $\alpha_1, \alpha_2, \ldots, \alpha_{\phi(n)}$ that are less than and coprime to n are congruent in some order to $r, r^2, \ldots, r^{\phi(n)}$ where r is a primitive root mod n

Since $(p-1)! = 1 \cdot 2 \ldots (p-1)$ and $1, 2, \ldots, (p-1)$ are smaller than and coprimt to n it follows that $(p-1)! \equiv r \cdot r^2 \ldots r^{\phi(n)} = r^{1+2+\ldots+(p-1)}$, which proves the hint

Using the hint and part (a) of question 5 and sum of first p natural numbers we can see that

$$(p-1)! \equiv r^{1+2+\ldots+(p-1)}$$
$$\equiv r^{\frac{p(p-1)}{2}} = \left(r^{\frac{p-1}{2}}\right)^p \equiv (-1)^p \equiv -1 \pmod{p}$$

which is wilson's theorem