Announcements: 1) Homework 7 solution is posted.

2) If you are registering for the course for the fall semester and would like to know your grade estimate based on your work so far, let me know.

3) We will try polling!

Proposition 1

proof: Among integers from 1 to p^k, those which are not relatively prime to p^k are $p, 2p, 3p, \ldots, p^k = p \cdot p^{k-1}$, and there are p^{k-1} such integers. Hence $\phi(p^k) = p^k - p^{k-1}$. $\square$

Theorem 2

proof: Using the multiplicative property, $\phi(n) = \phi(p_1^{k_1})\phi(p_2^{k_2}) \cdots \phi(p_r^{k_r})$. Using the above proposition, $\phi(p_i^{k_i}) = p_i^{k_i}(1 - \frac{1}{p_i})$. Therefore,

$$\phi(n) = p_1^{k_1}(1 - \frac{1}{p_1})p_2^{k_2}(1 - \frac{1}{p_2}) \cdots p_r^{k_r}(1 - \frac{1}{p_r}).$$

Factoring out all $p_i^{k_i}$'s and noting that $n = p_1^{k_1}p_2^{k_2} \cdots p_r^{k_r}$, we find that

$$\phi(n) = n\left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right) \cdots \left(1 - \frac{1}{p_r}\right).$$

hence proving the theorem. $\square$

1

Theorem 2: If $n = p_1^{k_1} p_2^{k_2} \cdots p_r^{k_r}$ is the prime decomposition of n, then

$$\phi(n) = n\left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right)\cdots\left(1 - \frac{1}{p_r}\right).$$

1552500 = 2^2 * 3^3 * 5^4 * 23

So ϕ(1552500) = 1552500 (1-(1/2)) * (1- (1/3)) * (1- (1/5)) * (1-(1/23))

=396000 relatively prime numbers

Cian

2

Update: Not sure what the exact wording of this problem was supposed to be. The way it's written it has was too many answers.

In addition to those listed here,i.e. n=625*p (p odd prime besides 5), and n=625*2^r, we can have

n=5^r*p where r>4 and p any odd prime besides 5 for which 4 does not divide p-1.

n=p^r*q^s*r^t where each of p,q,r =1 (mod 10) and r,s,t any powers.

n=p^r*q^s where p=1 (mod 100), q=1 (mod 10), and r,s are any powers.

On the other hand, if we ask when is phi(n)=1000, that has finitely many answers (see answer 2): https://math.stackexchange.com/questions/1282722/finite-or-infinite-n-in-%CF%86n

---

To have 3 0's at the end means the number is divisible by 1000, i.e. divisible by 2^3 and 5^3.

Note that phi(n) is a product of phi(p^k)'s and phi(p^k) is of the form p^{k-1}*(p-1), we can achieve the 5^3 factor by only choosing p=5, k=4.

In that case p-1=4 gives us 2^2. We need just one more 2 factor. This can come from another odd prime p (in (p-1)) or from p=2 with k>1.

So the numbers n must be of the form n=625*p (p<>5 odd prime) or =625*2^r with r>1.

?

You can check this with some n values at https://www.dcode.fr/euler-totient

Theorem 3

Fill in the blank in this proof is: $a^i = a^j * a^r * (a^d)^q = a^j * a^r \pmod{n}$

3 a,b

Find the order of 3 modulo 46. Explain your work.

46=2*23 so phi(46) = 46(1-1/2)(1-1/23) = 22. The order of 3 mod 46 must divide 22=2*11.

3^2 is not 1 mod 46 but 3^11 = 1 (mod 46) so the order of 3 mod 46 is 11.

Find the order of 5 modulo 357. Explain your work.

357 = 3*7*17 so phi(357) = 357(1-1/3)(1-1/7)(1-1/17) = 192. So the order of 5 mod 357 must divide 192 = 2^6 * 3.

Let d be the order of 5 mod 357. 5^(196/3) is not 1 mod 357 so 3 must be a factor of d. 5^(196/2) = 1 (mod 357) and 5^(196/4) = 1 (mod 357) but 5^(196/8) is not.

So d = 192/4 = 48 is the order of 5 mod 357.

-Nick

Order of 5^2 is 23, 5^{23} is 2, 5^3 is 46, 5^5 is 46.

Theorem 4

proof: We need to find what the product of all the numbers $1, 2, \ldots, (p-2), (p-1)$ are modulo p. We will consider the numbers $2, 3, \ldots, (p-2)$ separately from 1 and -1.

If x is one of $2, 3, \ldots, (p-2)$, then there is a unique y among $2, 3, \ldots, (p-2)$ such that $xy \equiv 1 \pmod{p}$ because each such x is invertible. Furthermore, for each such x, y pair, $y \neq x$ because $x^2 \equiv 1 \pmod{p}$ implies $x \equiv \pm 1 \pmod{p}$ (see homework solution problem 3 for how this follows). Therefore, each x among $2, 3, \ldots, (p-2)$ can be paired with a distinct y so that their product is 1.

When we consider $(p-1)!$ modulo n, most of the numbers can be paired to give 1. The only numbers which are not paired will be 1 and -1, so the whole product will be congruent to $1 \cdot (-1)$ modulo p, finishing the proof.

$\square$

5 a,b

a. If we let $x = 1*2*3*4*...*19*20$, then $x^2=-1$

b. We can use the same process with $x = ((p-1)/2)!$ as long as $(p-1)/2$ is even, which means $p-1=4*k$, i.e. $p=1+4k$.

Corollary 4

If p | M, then p | $4N^2+1$, so $4N^2+1=0$ (mod p), i.e. $4N^2=-1$ (mod p). This means (2N) is a solution to $x^2=-1$(mod p).

But that is a contradiction because we saw in Theorem 5 that for p=4k+3, there is no solution for $x^2=-1$ (mod p).

Why is 4 not a primitive root?

Suppose 4 is a primitive root. Then 2=4^k for some k < m, where m=phi(n), the order of 4. Since 4=2^2, taking square of both sides above, we get 4=2^2=4^(2k). So 4^(2k-1)=1.

This means that order of 4, m, divides 2k-1. But m is even (because phi(n) is even for every n) and 2k-1 is odd. Contradiction.

In next week's activity, we will learn how to determine which elements modulo n have square-roots using primitive roots, so that will also give us another way to think about this.

Last page