1

This is proposition 1 in the class activity.

2
a,b,c

2. For each of the following n, find $(n-1)!\pmod{n}$.

We could also say: for n=5 (n-1)!=4!=24=4 (mod 5) and for n=7 (n-1)!=6!=720=6 (mod 7)

a. $n = 5$
Since 5 is prime, then according to Wilson's Theorem $(n-1)! \equiv -1 \pmod{n}$

b. $n = 7$
Since 7 is prime, then according to Wilson's Theorem $(n-1)! \equiv -1 \pmod{n}$

c. $n = 10$
$(n-1)! = 9! = 9 \cdot 8 \cdot 7 \cdot 6 \cdot 5 \cdot 4 \cdot 3 \cdot 2 = 2 \cdot 5 \cdot q$ for some integer q due to the closure of integers under multiplication. Hence $9! \equiv 0 \pmod{10}$

Cy

2
d,e,f

(15-1)! =14! = 5*3*k=15k for some integer k. Thus, (15-1)! =0 (mod 15)

(17-1)! =16! =16*15*14*13*12*11*10 *9*8*7*6*5*4*3*2*1

Since we are working mod 17, to keep the numbers smaller we can change the first half of this list to be negatives.

This yields:
(-1)(-2)(-3)(-4)(-5)(-6)(-7)(-8)8*7*6*5*4*3*2*1 = (8!)^2 = (40320)^2 = (-4)^2 = 16 (mod 17)

(21-1)! =20! = 3*7*k=21k for some integer k. Thus, (21-1)! =0 (mod 21)

-Nick

3

Using the results of the previous problem, make a conjecture about $(n - 1)! \pmod n$ for composite $n > 4$ and prove it.

If n is a composite number which has no square numbers as a factor, then each of the prime factors of the number will appear only once, and will be less than n.

This means that (n-1)! will have at least one set of factors whose product will be n. This means that when we take the least residual of (n-1)! modulo n, we will get 0.

If n has multiple of the same prime factor, say n=(p_1^k_1)(p_2^k_2)(p_3^k_3)...(p_m^k_m), then for each p_i, there will be at least k_i p_i's in the prime factorization of (n-1)!.

We know this because for every k_i, p_i^k_i >= p_i * k_i. (The smallest p_i = 2, k_i = 1 .: 2^1 = 2 * 1; not a full proof, but we're using sticky notes).

So between 1 and p_i^k_i (which will be <= n), we will have at least k_i p_i's.

So again in this case, (n-1)! will have at least one set of factors whose product will be n, and so (n-1)! % n = 0.

- Miah :)

4

The order of any element divides p-1

and also p-1 always has order 2

There's another cool result (but a bit harder to see). Say order of a is k, even with k=2 (mod 4), then order of (-a) is k/2. If order of a is k, even with k=0 (mod 4), then order of (-a) is k.

Proof: If a has order even k: Then a^k=1 (mod p) and a^(k/2)=-1 (mod p) and no other a^r=-1.Then if k/2 is odd, (-a)^(k/2)=1 (mod p), so that's the order of (-a).

If k/2 is even, then (-a)^(k/2)=-1 (mod p) still, so the order of (-a) is still k.

If order of a is odd k, then order of (-a) is 2k. (Hmm.. I assumed this would be easier to prove, but I can't see it now. Left to the reader as an exercise.)

Num	1	2	3	4	5	6
order	1	3	6	3	6	2

mod 7

Num	1	2	3	4	5	6	7	8	9	10	11	12
order	1	12	3	6	4	12	12	4	3	6	12	2

mod 13

Cian

Last page