No announcements this week.

1 a

$7x \equiv 9 \pmod{15}$

First we set up the equation $7x = 9 + 15k$, or $7x - 15k = 9$.

Next we find $\gcd(7, 15) = 1$ as 7 is prime.

Reversing the euclidean algorithm gives us the solution that $1 = -2*7 + 1*15$. This also means that $9 = -18*7 + 9*15$. So we see that $x0 = -18 = -3 \equiv 12 \pmod{15}$.

Then we see that $xk = x0 + 15k/\gcd(7, 15) = x0 + 15k/1 = x0 + 15k \equiv x0 \pmod{15}$. So the solution is unique mod 15.

-Miah :)

1b

1. Let us now find solutions to each of the following equations using this idea. For each, find all integer solutions of the corresponding Diophantine equation and determine if your solution is unique with respect to the modulo you're working in.

   a. $7x \equiv 9 \pmod{15}$

   b. $9x \equiv 39 \pmod{42}$

$$9x - 39 = 42k$$
$$9x - 42k = 39.$$

Note that $\gcd(9, 42) = 3$ and $3 \mid 39$, so this equation has a solution. We express 3 as a linear combination of 9 and 42.

$$3 = (9 \cdot 5) - 42$$

We then multiply both sides by 13 to get

$$39 = 13(9 \cdot 5) - 13(42)$$

Expressed in mod, this means $9(13 \cdot 5) \equiv 39 \pmod{42}$. Which can be expressed more generally as $9(14n + 65) \equiv 39 \pmod{42}$ for some integer n.

1 c

We want to solve for 14x - 63 y = 42.

Note that by using Euclidean algorithm we can find gcd(14, 63)=7 (I mean, we can find it by trial and error too but we need a linear combination.)

63=4*14 + 7 and 14=2*7. So 7=63-4*14.

We then multiply both sides by 6 to get 42 as a linear combination: 42 = 6*63 - (4*6)*14.

So: (-24)*14 = 42 (mod 63), i.e. x=-24 is a solution. To find the other solutions, we add 63/7*k where k=0,1,...,6. Because this added term, when multiplied by 14, will become 0 mod 63.

We only go until 6 because x_0+9k and x_0+9k' will be equal mod 63 when 9(k-k') is divisible by 63.

2 a,b

The inverse of 5 (mod 14) is 3 because 3*5 = 15 and 15 is 1 (mod 14)

To solve for our x, we can see that 5x - 14k = 1 we can use 5(3) - 14(1) = 1. The next step is to multiply by 12 and get

5(36) - 14(12) = 12 so x should be 36. To find this mod 14 we do 36-14=22 and then 22-14=8 so x=8.

Nice use of "gcd as a linear combination" to solve for the inverse! So this is another reason why we want gcd=1 to find an inverse.

to check we do 5(8) mod 14 and see. 40 (mod 14) which is 26 (mod 14) which is 12 (mod 14) as desired

Once we have 5^(-1)=3, we could also use it to "cancel" 5 in 5x=12 (mod 14) by multiplying both sides by 5^(-1). So 5^(-1) essentially acts like dividing by 5.

That gives us: 5x=12 (mod 14) --> x=5^(-1)*12 (mod 14) --> x=36 (mod 14) --> x=8 (mod 14)

3 and corollary

Corollary: For a prime p, phi(p)= p-1. In other words, all numbers less then p are relatively prime to p.

3: For a prime p, p-1 residue classes have an inverse. (the ones not remainder 0)

The reason all p-1 residue classes have inverses is because

looking at ax==b (mod n)

If gcd(a,n) then the congruence ax==b (mod n) has a unique solution modulo n

So for all values of a, gcd(a, p) =1 and thus ax==1 (mod p) has a solution

Cian

When p, q are primes, what is phi(pq)?

For this we can use inclusion-exclusion. We will start with all numbers less than or equal to pq, remove the multiples of p, remove the multiples of q, then add back the multiples of pq.

The number of positive integers less than or equal to pq is pq.

Of these, the number of multiples of p is pq/p=q.

Similarly, the number of multiples of q is pq/q=p

Lastly the number of multiples of pq is pq/pq=1

Thus, phi(pq) = pq-q-p+1 = (p-1)(q-1)

Last page

Room 1 Names:

Solve for all x modulo 39101: 19337x=183 mod 39101

x = 38276 + 641k (mod 39101)

Agreed with your x definition. What is your k range?

1<=k<=61

Find the inverse of 45 mod 4579

The inverse of 45 is 4172

Room 2

$59 \cdot 461$ $\quad$ $59 \cdot 929$

b) $27199x \equiv 236 \pmod{54811}$

$54811 = 2 \cdot 27199 + 413$

$27199 = 65 \cdot 413 + 354$

$413 = 354 + 59$

$59 = 413 - 354 = 413 - (27199 - 65 \cdot 413)$

$= 66 \cdot 413 - 27199$

$= 66 \cdot 54811 - 133 \cdot 27199$

$236 = 59 \cdot 4 = 54811(66 \cdot 4) + 27199(-133 \cdot 4)$

$27199 \cdot (-532) \equiv 236 \pmod{54811}$

$-532, -532 + 929, \ldots, -532 + 929 \cdot 58$

I scanned the work for the first part of the work for Room 2 numbers just so we have another set of examples, and since I have it fully worked out, this could be helpful in other work.

2) a=47 n=4709 a^(-1)=-2104=2605 (mod 4709) (I don't have nicely written work for this.)

Room 3 Names:

- Miah :)

Cian

mirza

Joe

Solve for all x modulo 62779: 31289x= 268 mod 62779

x = 622 + 937k for any k

Find inverse of 47 modulo 4771.

The inverse is 4568.

Hmm.. yep, mine is equivalent to yours. I have -1252+937*k, but my k stops. What is your k range?

I have a negative one + a*k, so I'm trying to see if mine is equivalent to yours. How did you get the positive x?

Why would your k stop? even if it never repeated and say 2 mod 62779 was the only one you would get 2 + 62779 K

I'm looking for distinct solutions modulo 62779, so that's why I'm looking for a finite number of solutions.

OK, I think the other group is taking a bit long. So we won't reconvene as a whole group. We're all done with today. Week 7 stuff is up on Google drive already and I will post homework solution later today! Have a good evening.

k up from 0 to 66 are the unique ones????

ok