Breaking Down Number Theory Concepts into Simpler Steps

Note 1: These notes are intended to clarify the calculation process for the concepts introduced in Lecture 3: Number Theory and should therefore be used in conjunction with the slides not in lieu of them.

Note 2: There is not just one way to do these calculations (as you'll see in some of the additional resources at the end). If you end up finding a method that works better, makes more sense and gives the logical progression towards the final answer, then go forth and prosper.

Note 3: The best way to get to grips with these concepts is to practise them. Redo the worked examples in the slides so that you can check that you get the correct answer. Work through the additional examples at the end. Struggle through the calculations until you reach a result. If it's wrong, then try again, and again. In this case, it really is practise makes perfect.

How to compute the Greatest Common Divisor (GCD) using the Euclidean Algorithm

The Greatest Common Divisor (GCD) is the largest number that divides into both x and y. The Euclidean Algorithm allows one to find this number when factorising becomes difficult for very large numbers.

Given the question, find the gcd(x,y):

1. First calculate y/x and write down the whole number result z.
2. Subsequently, the first part of your answer becomes z * x
3. Calulate the modulus y mod x by subtracting the whole number z from the result of y/x. Multiply this result by x.
4. Subsequently, the tail end of your answer becomes the result of + [(y/x)-z] * x. This is the modulus value (or the remainder if you were doing long division).
5. The answer for your first iteration of the Euclidean algorithm becomes y= z * x + y mod x. Remember, z is the whole number from y/x.
6. In the next iteration of the algorithm, the x becomes the new y and [y mod x] becomes the new x
7. Repeat steps 1 to 6 until you get a remainder of 1.
8. At this point, your result at y mod x=1 is the gcd(x,y)

Worked Example: Find the gcd(79, 3220)

To start off, express that x=79, y=3220. This is the information that is given from the question.

[Start iteration 1]

1. Calculate that 3220/79= 40.7594… (Here the whole number z=40)
2. Part 1 of your answer is therefore found to be 40 * 79 (z * x)
3. Calculate the remainder y mod x= 3220 mod 79
   = 40.7594… - 40 *subtract the whole number z*
   = 0.7594936709 x 79 *multiply by x*
   = 60
4. Part 2 of your answer is therefore y mod x= 3220 mod 79=60
5. Therefore the first iteration (y= z*x + y mod x) of the algorithm is 3220=40*79+60
6. From this, for the next iteration, the x of the current iteration becomes the new y (79) and the remainder of the current iteration becomes the new x (60)

[Repeat steps 1-6 for iteration 2]

1. 79/60=1.316666667
2. z=1, therefore part 1 of answer becomes 1*60
3. 79 mod 60= 1.316666667 -1 * 60 =19
4. Part 2 of answer is y mod x= 79 mod 60= 19
5. Therefore 79= 1*60+19
6. For next iteration, y=60, x=19

[Repeat steps 1-6 for iteration 3]

1. 60/19=3.157894737
2. z=3, therefore part 1 of answer becomes 3*19
3. 60 mod 19= 3.157894737-3 * 19 =3
4. Part 2 of answer is y mod x= 60 mod 19=3
5. Therefore 60= 3*19+3
6. For next iteration, y=19, x=3

[Repeat steps 1-6 for iteration 4]

1. 19/3=6.33333333333
2. Z=6, therefore part 1 of answer becomes 6*3
3. 19 mod 3= 6.33333333333-6 * 3 =1
4. Part 2 of answer is y mod x= 19 mod 3=1
5. Therefore 19= 6*3+1

At this step, you can see that y mod x = 1. Rearrange the equation result such that 1 is the subject of the equation (1 should become the y). You end up with 1=19-6*3 and you stop. You have thus found that the gcd(79,3220)=1=19-6*3.

Note: Remember to write the gcd with the small number first in the brackets

How to calculate the Modular Inverse (Extended Euclidean)

The modular inverse occurs when you have two intergers *x* and *y* which, when multiplied together, give you the result of 1 modulo *n*; i.e. *x***y* ≡ 1 mod *n*. The integers *x* and *y* are said to be multiplicative inverses of modulo *n*. What is important to note is that an integer x will only have an inverse modulo *n*, if and only if, the greatest common divisor is equal to one (gcd(x,n)=1). If the gcd(x,n)>1, there is no inverse modulo *n*. *Source: https://www.youtube.com/watch?v=FnQNbFl72LY*

To find the modular inverse, the extended Euclidean algorithm is used. Picking up from the end of the previous section, once you have found the gcd, you start to work backwards in order to find the modular inverse (this will sound confusing but will make more sense in a worked example):

1. Re-arrange equation such that 1=y-z*(x). This is where we left off for the gcd calculation
2. Substitute into *x*, the equation value for x from the preceeding step in the gcd calculation
3. Multiply in *z* but keep the full operations unsimplified i.e don't multiply out just yet
4. Factor out the remainder value from the preceeding gcd step. This is to ensure it can be replaced with its equation equivalent
5. Group together the whole numbers not featuring in the preceeding gcd calculation and simplify
6. Rearrange the result such that the factored out remainder value becomes the new x value (the last multiply term in the equation)

7. Repeat steps (2) to (6) until back at the original x and y values. At this stage you should have something to the effect of 1= a x (original gcd y value) + b x (original gcd x value).
8. Re-arrange terms again such that the y term from the initial gcd question is to the right.

   1= b x (original gcd x value) + a x (original gcd y value)
9. Change the equals sign between 1 and the equation to a congruence sign
10. Modular y all terms.

    1 (mod y) ≡ b x (original gcd x value) [mod y] + a x (original gcd y value) [mod y]
11. y mod y is equals to zero (from modular arithmetic) so that term falls away. You end up left with b * x mod y ≡ 1 mod y
12. Once in this form, the modular inverse is the multiple value (b) for the x term.

Worked example: Find the modular inverse of 79 mod 3220 i.e 79^{-1} mod 3220

From the previous section, the calculation of gcd(79,3220) was found to be:

(1) 3220=40*79+60
(2) 79=1*60+19
(3) 60=3*19+3
(4) 19=6*3+1

The red highlighted numbers are the factors that will need to be taken out and replaced with equations

1. 1=19-6*(3) *Rearrange equation. 3 is the remainder value from (3)*
2. =19-6*(60-3*19) *Substitute in 3=60-3*19 from preceeding gcd step*
3. =19-6*60+6*3*19 *write out whole equation after mutiplying in*
4. =- 6*60 +19(1+ 6*3*1) *factor out such that factors is the a and b values (60 and 19) for (3)*
5. =-6*60 +19 *19 *rearrange result to have the remainder from the preceeding gcd calculation (in this case (2)) as the last multiply term in the equation*

[Repeat]

1. 1=-6x60*+19(19) *Rearrange equation. 19 is the remainder value from (2)*
2. =-6x60 +19(79-1x60) *Substitute in 19=79-1x60 from preceeding gcd step*
3. =-6x60+19x79-1x60x19 *write out whole equation after mutiplying in*
4. =60(-6-1x19) + 19x79 *factor out such that factors is the a and b values (60 and 79) for (2)*
5. =19x79 -25 x60 *rearrange result to have the remainder from the preceeding gcd calculation (in this case 1) as the last multiply term in the equation*

[Repeat]

1. 1=19x79-25*(60) *Rearrange equation. 60 is the remainder value from (1). This is the top of the gcd calculation and therefore the last repetition*
2. =19x79-25(3220-40x79) *Substitute in 60=3220-40x79 from preceeding gcd step*
3. =19x79-25x3220+25x40x79 *write out whole equation after mutiplying in*
4. =79(19+40x25) -25x3220 *factor out such that factors is the a and b values (3220 and 79) for (1)*
5. 1=-25x3220 + 1019x79 *rearrange result to have the remainder from the preceeding gcd calculation as the last multiply term in the equation*

6. No more repetitions at this point because we are now back to the starting x and y values. To find the modular inverse value:
7. 1019 x79 -25x3220 ≡ 1 *Re-arrange terms so that the y term from the initial gcd question is to the right. Change equals sign to congruence sign*
8. 1019x79 mod 3220 -25x3220 mod 3220 ≡ 1 mod 3220 *Mod everything with the y term (in this case 3220)*
9. 1019x79 mod 3220 ≡ 1 mod 3220 *a x y mod y falls away. You end up left with this result*

10. Therefore the modular inverse of 79 mod 3220 (79^{-1} mod 3220) is 1019. *Once in this form, the modular inverse is the multiple value *b* for the *x* term*

How to calculate using Modular Exponentiation (Square/Multiply)

Modular exponentiation allows for the simplification of large exponents down to smaller, more managable numbers in order to be able to calculate the modulus. The square-multiply method relies on dividing the large exponent into multiples of the powers of 2 and using the modulus of the squared values to calculate the modulus of the higher powers.

To do square/multiply modular exponentiation:

1. Take the exponent and break it up into additions of its factors as powers of 2.
2. Using exponent arithmetic, expand out into the multiples of powers of 2.
3. Calculate the modulus of square value.
4. Calculate the modulus of higher powers of 2 values using the modulus value calculated for the squared value
5. Select the modulus value for the exponent multiples (from step 2) in order to calculate the final modulus as sometimes you calculate for modulus values than is required for the exponent.
6. Multiply all values to get the simplified result of the modular exponetiation equation.
7. Calculate the modulus as normal to get the final answer

Worked example: Solve 11^{15} mod 13 using modular exponentiation

1. 15=8+4+2+1 *separate exponent into powers of 2*
2. $11^{15}= 11^{8+4+2+1}=11^8$ x 11^4 x 11^2 x 11^1 *use exponent arithmatic to divide into powers of 2*
3. 11^2 mod 13= 121 mod 13= 4 *calculate modulus of square value*
4. 11^4 mod 13 = (11^2mod 13)^{2}mod 13 =$(4)^2$ mod 13 = 16 mod 13 =3 *use the modulus of 11^2 to calculate*
   11^8 mod 13= (11^4mod 13)^2 mod 13= $(3)^2$ mod 13= 9 mod 13 =9 *use the modulus of 11^4 to calculate*
5. For 11^{15}, you need the values for 11^8 (9), 11^4 (3), 11^2 (4) *select modulus values needed to calculate final modulus*
6. 11^{15} mod 13 = (9 x 3 x 4 x 11) mod 13 *use the modulus answers to get the simplified value*
7. =1188 mod 13 = 5 *calculate modulus to get final answer*

How to use Femat's Little Theorem and Euler's phi Function

Femat's Little Theorem is to be used together with Euler's phi function. Femat's Little Theorem states:

Given a number (*a*) raised to a power (*p-1*) where *p* is a prime number…
$a^{p-1} \equiv 1$ (mod p) *When a^{p-1} is divided by *p*, you get a remainder of 1.*

Conditions for this to work: You need to have an integer *a* where **a is not a multiple of p**; i.e. a is **not** divisible by p

Worked mini example: Setting up Femat's Little Theorem

Given 2^{16}…
a=2, p-1=16 therefore p=17

$2^{17-1} \equiv 1 \pmod{17}$
$2^{16} \equiv 1 \pmod{17}$
$2^{16} \bmod 17 \equiv 1$

When combining Femat's Little Theorem with Euler's phi funtion…

$\phi(mn)= \phi(m) \times \phi(n)$ for gcd(m,n)=1

$\phi(p^e)= p^{e-1} (p-1)$ for a prime p and exponent $e \geq 1$

Therefore, if $n = p_1 * p_2 * p_{3\ldots} * p_k$ then $\phi(n) = \phi(p_1)*\phi(p_2)*\phi(p_3)\ldots*\phi(p_k)$

We can write this as alternative equation
$\phi(n)= n(1- 1/p_1)*(1-1/p_2)*(1-1/p_3)\ldots(1-1/p_k)$ [non-prime number] *When p is a non-prime number, break it down into its sum of prime numbers. These then form p_1, p_2, $p_3\ldots p_k$*

or

$\phi(n)$=p-1 [prime number]

Euler's generalisation says that: should n be a composite integer (an integer able to be divided up into a series of prime numbers), then $a^{\phi(n)} \equiv 1 \pmod{n}$

Worked example: Calculate 39^{191} mod 47

39^{191} mod 47 can be seen to be in the form $a^{\phi(n)}$ mod n from Euler's generalisation.
Therefore, a=39, n=47

From this, $\phi(n)$ can be calculated…

$\phi(47)$= p-1 *n=47 and 47 is prime therefore prime number equation can be used*
$\phi(47)$= 47-1 =46
$39^{46} \equiv 1$ mod 47 *By Euler's totient function*
Find the highest multiple of 46 closest to 191, the original exponent
46*2=92; 46*3=138, 46*4=184, 46*5=230 (184 is the closest to 191)
subtract the highest multiple from the original exponent
191-184=7
Therefore 191= 184 + 7
Going back to the original exponent, simplify by spliting it into the composite exponents
$39^{191}= 39^{184+7}= 39^{184} \times 39^7$ *exponent arithmetic*

Now calculate the original modulus
39^{191} (mod 47) = 39^{184} mod 47 x 39^7 mod 47
= $(39^{46})^4$ mod 47 x 39^7 mod 47 *replace 39^{184} with its 39^{46} equivalent. Remember, we found that 184 was a multiple of 46 earlier in the calculation*

$= (1)^4 \times 39^7 \bmod 47$ *value of $39^{46} \bmod 37$ was seen to be 1 using Euler's totient earlier*

$=39^7 \bmod 47$ *now modulus is simplified down to a smaller value. Calculate using modular exponentiation (square/multiply) as 39^7 is still too big for some calculators*

[Divert here to modular exponentiation calculation]

$7= 2^2 + 2^1 + 2^0= 4 + 2 + 1$ *Divide the exponent into powers of 2*

$39^7=39^{4+2+1}= 39^4 \times 39^2 \times 39^1$

$39^2 \bmod 47=1521 \bmod 47=17$ *calculate the modulus of the square value*

$39^4 \bmod 47= (39^2)^2 \bmod 47= (17)^2 \bmod 47 =289$ *use the result of the square value modulus to calculate the modulus of $39^4 \bmod 47$*

[Go back to original modulus equation using values calculated using modular exponentiation]

$39^7 \bmod 47 = (39^4 \bmod 47 \times 39^2 \bmod 47 \times 39) \bmod 47$

$= (289 \times 17 \times 39) \bmod 47$ *substitute in the values for the powers of 2 that were calculated previously*

$= 191607 \bmod 47$ *calculate modulus as normal to get final answer*

$= 35$

Therefore $39^{191} \equiv 191607 \bmod 47 \equiv 35$.

Some Additional Video Resources

Note: There are many other resources on the internet that can help with understanding these number theory concepts. The list below is just a small number of available resources.

Basic Modular Artihmetic funtions : https://www.youtube.com/playlist?list=PL1ZN4kabqbof_aDUyIcD6tQntun8LLIgL

Modular Exponentiation: https://www.youtube.com/watch?v=tTuWmcikE0Q

Modular Inverse and GCD: https://www.youtube.com/watch?v=mgvA3z-vOzc

Femat's Little Theorem: https://www.youtube.com/watch?v=pMA-dD-KCWM&t=331s ; https://www.youtube.com/watch?v=oT7kRlh1nVQ

Euler's phi funtion: https://www.youtube.com/watch?v=qa_hksAzpSg

Euler's Totient function: https://www.youtube.com/watch?v=FHkS3ydTM3M&t=225s