UNIVERSITY OF WATERLOO

Faculty of Mathematics
Waterloo, Ontario N2L 3G1

Centre for Education in
Mathematics and Computing

Grade 7/8 Math Circles

February 23-24, 2016

Number Theory

Greatest Common Divisors are very useful in the math world, used in multiple branches in math. It is also the basics of Number theory, which may seem intimidating at first, but I promise it really isn't, and you'll see a little bit of it today.

Let's start by calculating the GCD of a few pairs of numbers by using prime factorization.

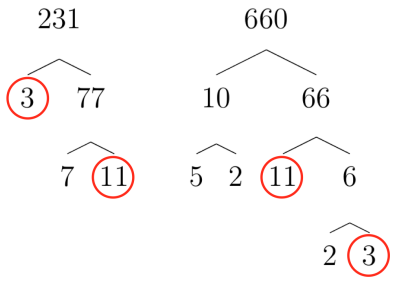
Do you remember what a prime number is?

It is basically any number whose divisors are only 1 and itself, or in other words it is not a multiple of any other number.

So in this section all we will do is write really big numbers in terms of a product of prime numbers. The first few prime numbers are $2, 3, 5, 7, 11, 13, ...$

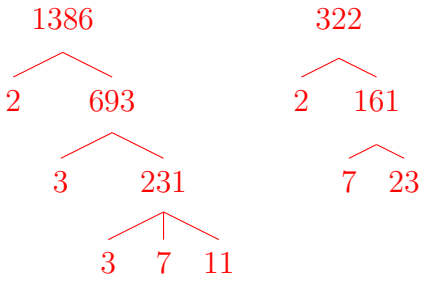
Example 1

(a) Find the GCD of 231 and 660



So, $\gcd(231, 660) = 3 \times 11 = 33$

(b) Find the GCD of 1386 and 322



So, $\gcd(1386, 322) = 2 \times 7 = 14$

Now, how annoying was that? Like what if you just can't think of a factor, and every number less than 20 doesn't divide it? It would be quite annoying just using guess and check right? So mathemticians have come up with an algorithm (basically a big word for bunch of steps) to compute this in a much more organized and logical way. But, before we jump into that, let's do a quick review of modular arithmetic.

1 Review of Modular Arithmetic

Remember: $a \pmod{n} = r$ means that when a is divided by n, there is a remainder of r. So, $7 \pmod{3} = 1$ since $7 = 2(3) + 1$ where 2 is the quotient and 1 is the remainder, and $15 \pmod{4} = 3$ since $15 = 3(4) + 3$.

Example 2

(a) $234 \pmod{4} = 2$ since $234 = 58(4) + 2$.

(b) $478 \pmod{6} = 4$ since $478 = 79(6) + 4$.

(c) $582 \pmod{9} = 6$ since $582 = 64(9) + 6$.

(d) $679 \pmod{8} = 7$ since $679 = 84(8) + 7$.

2 Euclidean Algorithm

The Euclidean algortihm is used to solve for the GCD of any 2 integers.
We write $d = \gcd(a, b)$, where a and b are the integers we're given in the question.
The algorithm is pretty simple, you start by computing $a \pmod{b}$ and call that r_1. Then compute $b \pmod{r_1}$ and call that r_2. Keep repeating this until the remainder is zero, at which point you know that the GCD of a and b is the remainder on the second last line.

For example, let's compute the GCD of 660 and 231 using the Euclidean Algorithm.

$$r_1 = 660 \pmod{231} = 198$$
$$r_2 = 231 \pmod{198} = 33$$
$$r_3 = 198 \pmod{33} = 0$$

How much easier was that? Absolutely no guessing and checking factors, only 2 remainders and you're done! *Obviously it won't always be 2, sometimes more, but still so much easier.*

Example 3
Calculate the GCD of each of the following pairs of numbers.

(a) $\gcd(1386, 322) = 14$
$1386 \pmod{322} = 98$
$322 \pmod{98} = 28$
$98 \pmod{28} = 14$
$28 \pmod{14} = 0$

(b) $\gcd(111, 11111) = 1$
$11111 \pmod{111} = 11$
$111 \pmod{11} = 1$
$11 \pmod{1} = 0$

(c) $\gcd(442, 289) = 17$
$442 \pmod{289} = 153$
$289 \pmod{153} = 136$
$153 \pmod{136} = 17$
$136 \pmod{17} = 0$

(d) $\gcd(435, 377) = 29$
$435 \pmod{377} = 58$
$377 \pmod{58} = 29$
$58 \pmod{29} = 0$

There's just one problem - we often also want 2 numbers x and y such that:

$$ax + by = d \text{ where } d = \gcd(a, b)$$

Mathmaticians have extended the Euclidean Algorithm so finding these 2 integers would be very easy.

3 Extended Euclidean Algorithm

It uses a simple 4-column table and a repetitive use of remainders (r) and quotients (q) and gives us not only the GCD but also an x and y such that $ax + by = d$.
We start the table off like this, placing the larger number on top:

x	y	r	q
1	0	a	0
0	1	b	0

Then, like before we will calculate $a \pmod b = r_1$ and place it underneath b like this:

x	y	r	q
1	0	660	0
0	1	231	0
		198	

Next we want to calculate the quotient when 660 is divided by 231, and let that be q_3, (write that in the q column, in the 3^{rd} row).

x	y	r	q
1	0	660	0
0	1	231	0
		198	2

Then in each of the first two columns, calculate $Row_1 - (q_3 \times Row_2)$

x	y	r	q
1	0	660	0
0	1	231	0
1	-2	198	2

Now, just like the Euclidean algorithm, you repeat these 3 steps until you get a remainder of 0. The second last row provides the desired x, y and d.

x	y	r	q
1	0	660	0
0	1	231	0
1	-2	198	2
-1	3	33	1
7	-20	0	6

So, 33 is the GCD of 660 and 231. Also $(-1 \times 660) + (3 \times 231) = 33$.

Example 4

(a) $\gcd(1386, 322) = 14$

x	y	r	q
1	0	1386	0
0	1	322	0
1	-4	98	4
-3	13	28	3
10	-43	14	3
-23	99	0	2

$\therefore 10(1386) - 43(322) = 14$

(b) $\gcd(111, 11111) = 1$

x	y	r	q
1	0	11111	0
0	1	111	0
1	-100	11	100
-10	1001	1	10
111	-11111	0	11

$\therefore -10(11111) + 1001(111) = 1$

4 Coprimes

Remember that primes are number whose only factors are 1 and itself.
Similarily, 2 integers are *coprimes* if the only integer which evenly divides both of them is 1
Think of it as COMMON *factors. The only common factor is 1.*
For example, 4 and 9 are coprimes since the prime factorization of 4 and 9 are $4 = 2 \times 2$ and $9 = 3 \times 3$ respectively, so they have no common factors.
Connection: If we were to apply the Euclidean Algorithm or the Extended Euclidean Algorithm to 2 coprime numbers, what should the GCD come out to be? 1

Example 5
Determine which of the following pairs of numbers are coprimes.

(a) 15 and 18
$\gcd(15, 18) = 3$
$\implies$ they are NOT coprime.

(b) 19 and 21
$\gcd(19, 21) = 1$
$\implies$ they are coprime.
(which is obvious since 19 is prime)

(c) 16 and 25
$\gcd(16, 25) = 1$
$\implies$ they are coprime.

(d) 36 and 45
$\gcd(36, 45) = 9$
$\implies$ they are NOT coprime.

(e) 46 and 55
$\gcd(46, 55) = 1$
$\implies$ they are coprime.

5 Exponent Laws

Before we start the next section, we need to review a few exponent laws.

(a) When multiplying numbers with the same base, add the exponents: $b^x \times b^y = b^{x+y}$

(b) When raising a exponential to an exponent, multiply the exponents: $(b^x)^y = b^{x \cdot y}$

6 Fermat's Little Theorem

Let p be a prime and a be a positive integer not divisible by p. Then,

$$a^{p-1} \pmod{p} = 1 \tag{1}$$

For example, $5^6 \pmod 7 = 15625 \pmod 7 = (2232 \times 7) + 1 \pmod 7 = 1$.
Multiplying each side by a we get that

$$a^p \pmod{p} = a \tag{2}$$

However, it is cricital to note these are only necessarily true if $p \nmid a$.
But if $p \mid a$ what is $a^x \pmod p$ equal to, for any integer x? __0__.

Example 6

(a) $3^7 \pmod 7 = 3$

(b) $29^{10} \pmod{11} = 1$

(c) $28^{17} \pmod{17} = 28$

Now, that was pretty easy right? As long as $p \nmid a$ and the exponent is either p or $p-1$ we know the answer will either be a or 1.
But what if we were asked to calculate $3141^{2001} \pmod{17}$? Could we use Fermat's Little Theorem to simplify this a little? *Turns out we can!*
Remember that $(x \times y) \pmod p = [x \pmod p \times y \pmod p] \pmod p$.
A similar property holds with exponents: $x^y \pmod p = [x \pmod p]^y$.
As an aside: Why is that so?
Since exponentiation is just repetitive multiplication, if $a \pmod p = b$ *then*
$a^k \pmod p = (a \pmod p)^k = (b \pmod p)^k$

So first step is we want to calculate $3141 \pmod{17}$ which turns out to be:

$$3141 \pmod{17} = 13$$

and we know by Fermat's Little Theorem that,

$$a^{16} \pmod{17} = 1$$

when $17 \nmid a$. Putting all of this together, we get

$$3141^{2001} \pmod{17} = 13^{(125\times16)+1} \pmod{17} = (13^{16})^{125} \times 13^1 \pmod{17} = 1^{125} \times 13 = 13$$

Example 7: Fill out the following table.

k	1	2	3	4	5
$1^k \pmod 5$	1	1	1	1	1
$2^k \pmod 5$	2	4	3	1	2
$3^k \pmod 5$	3	4	2	1	3
$4^k \pmod 5$	4	1	4	1	4

What patterns do you see? Why is that the case?
Notice: the 4^{th} column is all 1's since 5 doesn't divide any number between 2 and 4, and so by Fermat's Little Theorem, $a^4 \pmod 5 = 1$ (for $a = 2, 3,$ or 4).
Also, the last column is just the base itself *(ie. 1, 2, 3 and 4 in that order)* by the second part of Fermat's Little Theorem.
Lastly, the last row alternates between 1 and 4. This is due to the fact that 4 is also equivalent to $-1 \pmod 5$ so $(-1)^2 \pmod 5 = 1$ but $(-1)^3 \pmod 5 = -1 \pmod 5 = 4$.

7 Just for fun: Cyclic Numbers

A cyclic number is a number of n digits which when it is multiplied by $1, 2, 3, 4, ..., n$ all the digits remain the same and in the same order just rotated in a circular fashion!
The smallest cyclic number is 142857.
Notice that if you multiply it by any number greater than 6, the number of digits in the cyclic number, it will not follow the same pattern.
There are 4 main properties of cyclic numbers:

1. When you multiply it by $1, \ldots, n$ you get the same digits rotating in a circular fashion.

$$142857 \times 1 = \underline{1}42857$$
$$142857 \times 2 = 285714$$
$$142857 \times 3 = 428571$$
$$142857 \times 4 = 571428$$
$$142857 \times 5 = 714285$$
$$142857 \times 6 = 857142$$

2. When you multiply it by $n + 1$ you get a string of 9's of length n.

$$142857 \times 7 = 999999$$

3. Sum of the m-digit substrings of the cyclic number is a string of m 9's.

$$14 + 28 + 57 = 99$$
$$142 + 857 = 999$$

4. Difference of squares (using the digits in order) equals the original number, perhaps rotated.

$$857^2 - 142^2 = 714285$$
$$571^2 - 428^2 = 142857$$
$$714^2 - 285^2 = 428571$$

8 Problem Set

1. Calculate the GCD of each of the following pairs of numbers, using the Euclidean Algorithm.

   (a) $\gcd(442, 289) = 17$
   $442 \pmod{289} = 153$
   $289 \pmod{153} = 136$
   $152 \pmod{136} = 17$
   $136 \pmod{17} = 0$

   (b) $\gcd(435, 377) = 29$
   $435 \pmod{377} = 58$
   $377 \pmod{58} = 29$
   $58 \pmod{29} = 0$

   (c) $\gcd(480, 1800) = 120$
   $1800 \pmod{480} = 360$
   $480 \pmod{360} = 120$
   $360 \pmod{120} = 0$

   (d) $\gcd(273, 595) = 7$
   $595 \pmod{273} = 49$
   $273 \pmod{49} = 28$
   $49 \pmod{28} = 21$
   $28 \pmod{21} = 7$
   $21 \pmod{7} = 0$

   (e) $\gcd(9081, 3270) = 3$
   $9081 \pmod{3270} = 2541$
   $3270 \pmod{2541} = 729$
   $2541 \pmod{729} = 354$
   $729 \pmod{354} = 21$
   $354 \pmod{21} = 18$
   $21 \pmod{18} = 3$
   $18 \pmod{3} = 0$

2. Calculate the GCD of each of the following pairs of numbers, and find integers a and b such that $ax + by = d$, using the Extended Euclidean Algorithm.

(a) $\gcd(36, 150) = 6$

x	y	r	q
1	0	150	0
0	1	36	0
1	-4	6	4
-6	25	0	6

$\therefore 1(150) - 4(36) = 6$

(b) $\gcd(442, 289) = 17$

x	y	r	q
1	0	442	0
0	1	289	0
1	-1	153	1
-1	2	136	1
2	-3	17	1
-17	26	0	8

$\therefore 2(422) - 3(289) = 17$

(c) $\gcd(144, 720) = 144$

x	y	r	q
1	0	720	0
0	1	144	0
1	-5	0	5

$\therefore 0(720) + 1(144) = 144$

(d) $\gcd(60, 1764) = 12$

x	y	r	q
1	0	1764	0
0	1	60	0
1	-29	24	29
-2	59	12	2
5	-147	0	2

$\therefore -2(1764) + 59(60) = 12$

(e) $\gcd(204, 22050) = 12$

x	y	r	q
1	0	22056	0
0	1	204	0
1	-108	24	108
-8	865	12	8
17	-1738	0	0

$\therefore -(22056) + 865(204) = 12$

(f) $\gcd(11550, 36) = 6$

x	y	r	q
1	0	11550	0
0	1	36	0
1	-320	30	320
-1	321	6	1
6	-1925	0	5

$\therefore -1(11550) + 321(36) = 6$

3. Which of the following pairs of numbers are coprime?

   (a) 6 and 25

   Yes, they are coprime since $\gcd(6, 25) = 1$

   (b) 12 and 21

   No, they are not coprime since $\gcd(12, 21) = 3$

   (c) 16 and 27

   Yes, they are coprime since $\gcd(16, 27) = 1$

   (d) 15 and 28

   Yes, they are coprime since $\gcd(15, 28) = 1$

   (e) 30 and 42

   No, they are not coprime since $\gcd(30, 42) = 6$

   (f) 105 and 42

   No, they are not coprime since $\gcd(105, 42) = 21$

4. Calculate each of the following.

   (a) $11^4 - 1 \pmod 5$
   $= 1 - 1 \pmod 5$
   $= 0$

   (b) $3^{50} \pmod 7$
   $= 3^{48} \cdot 3^2 \pmod 7$
   $= (3^6)^8 \times 9 \pmod 7$
   $= 1 \times 2 = 2$

   (c) $3^{70} \pmod{67}$
   $= 3^{70} \pmod{67}$
   $= 3^{66} \times 3^4 \pmod{67}$
   $= 1 \times 81 \pmod{67}$
   $= 14$

   (d) $2^{345} \pmod{11}$
   $= (2^{10})^{34} \times 2^5 \pmod{11}$
   $= 1^{34} \times 32 \pmod{11}$
   $= 1 \times 10 \pmod{11}$
   $= 10$

   (e) $9^{794} \pmod{73}$
   $= (9^{72})^{11} \times 9^2 \pmod{73}$
   $= 1 \times 81 \pmod{73}$
   $= 8$

   (f) $2^{2007} \pmod{15}$
   $= (2^{14})^{143} \times 2^5 \pmod{15}$
   $= 1 \times 32 \pmod{15}$
   $= 2$

5. What is the last digit of 4321^{4321}?

   To figure out the last digit of any number all we need to do is calculate the number modulo 10, like this:

$$\begin{aligned} & 4231^{4321} \pmod{10} \\ &= [1 \pmod{10}]^{432(10)+1} \\ &= [(1^{10})^{432} \pmod{10}] \cdot [1^1 \pmod{10}] \\ &= 1 \end{aligned}$$

   $\therefore$ The last digit of 4321^{4321} is 1.

6. Fill out the following table.

k	1	2	3	4	5	6	7
$1^k \pmod 7$	1	1	1	1	1	1	1
$2^k \pmod 7$	2	4	1	2	4	1	2
$3^k \pmod 7$	3	2	6	4	5	1	3
$4^k \pmod 7$	4	2	1	4	2	1	4
$5^k \pmod 7$	5	9	6	2	3	1	5
$6^k \pmod 7$	6	1	6	1	6	1	6