Number Theory Class 1

Lucas Brown

Saturday, 26 September 2009

1 The book

Buy Mathew Crawford's *Introduction to Number Theory* at www.artofproblemsolving.com.

2 Integers: The Basics

Integers are numbers that have no fractional part. The set of all integers is often denoted $\mathbb{Z}$.

Whole numbers are non-negative integers. The set of all whole numbers is often denoted $\mathbb{W}$.

Natural numbers are positive integers. The set of all natural numbers is often denoted $\mathbb{N}$.

In number theory, we are primarity concerned with natural numbers and equations whose only solutions we care about are natural numbers ("Diophantine" equations). This restriction can sometimes be aggravating. For example, finding integral solutions to $x + y = 4171$ is easy while finding integral solutions to $xy = 4171$ is an entirely different matter. The additive equation has an infinite number of solutions, and each integral value of x (or y) will give a corresponding integer for y (or x) that will solve the equation. The multiplicative equation, on the other hand, has exactly 8 pairs (x, y) that will satisfy it: $(1, 4171)$, $(43, 97)$, $(97, 43)$, $(4171, 1)$, and their negatives. The reason is that the *prime factorization* of 4171 is $43 * 97$. Prime factorization is an extremely important topic of number theory, but before we can discuss it, we must define a few things.

3 Some definitions

3.1 Divisibility

Formally, x divides y iff (”if and only if”) $\frac{y}{x}$ is an integer, and x does not divide y iff $\frac{y}{x}$ is not an integer. Symbolically, we may write

$$x \mid y \leftrightarrow \frac{y}{x} \in \mathbb{Z}$$

and

$$x \nmid y \leftrightarrow \frac{y}{x} \notin \mathbb{Z} \tag{1}$$

The vertical bar means “divides,” the double-headed arrow means “iff,” $\in$ means “is an element of,” and $\notin$ means “is not an element of.”

Divisibility is transitive but not commutative, and associativity does not apply.

3.2 Divisor

x is a divisor of y iff $x \mid y$ - that is, iff $\frac{y}{x} \in \mathbb{Z}$.

3.3 Multiple

y is a multiple of x iff x is a divisor of y.

3.4 Composites

A composite number is a number that has positive divisors other than 1 and itself. The first ten composites are 4, 6, 8, 9, 10, 12, 14, 15, 18, and 20.

4 Prime numbers

A prime number p (an element of $\mathbb{P}$) is a number that has no positive divisors except for 1 and itself. The first ten are 2, 3, 5, 7, 11, 13, 17, 19, 23, and 29. 1 is generally not considered prime.

4.1 The Sieve of Eratosthenes

Eratosthenes was an ancient Egyptian mathematician who is most well-known today for calculating the circumference of the Earth. However, it is his namesake “sieve” - a method of making a list of primes - that interests us. The sieve is generated as follows.

1. List as many integers as you want, starting with 2 and not skipping any.

	2	3	4	5	6	7	8	9	10
11	12	13	14	15	16	17	18	19	10
21	22	23	24	25	26	27	28	29	10
31	32	33	34	35	36	37	38	39	10
41	42	43	44	45	46	47	48	49	10
51	52	53	54	55	56	57	58	59	10
61	62	63	64	65	66	67	68	69	10
71	72	73	74	75	76	77	78	79	10
81	82	83	84	85	86	87	88	89	10
91	92	93	94	95	96	97	98	99	100

2. Find the smallest unmarked number. Mark it somehow; here, we will box it.

	$\boxed{2}$	3	4	5	6	7	8	9	10
11	12	13	14	15	16	17	18	19	20
21	22	23	24	25	26	27	28	29	30
31	32	33	34	35	36	37	38	39	40
41	42	43	44	45	46	47	48	49	50
51	52	53	54	55	56	57	58	59	60
61	62	63	64	65	66	67	68	69	70
71	72	73	74	75	76	77	78	79	80
81	82	83	84	85	86	87	88	89	90
91	92	93	94	95	96	97	98	99	100

3. Mark all multiples of the number in a different way. We will italicize.

	$\boxed{2}$	3	*4*	5	*6*	7	*8*	9	*10*
11	*12*	13	*14*	15	*16*	17	*18*	19	*20*
21	*22*	23	*24*	25	*26*	27	*28*	29	*30*
31	*32*	33	*34*	35	*36*	37	*38*	39	*40*
41	*42*	43	*44*	45	*46*	47	*48*	49	*50*
51	*52*	53	*54*	55	*56*	57	*58*	59	*60*
61	*62*	63	*64*	65	*66*	67	*68*	69	*70*
71	*72*	73	*74*	75	*76*	77	*78*	79	*80*
81	*82*	83	*84*	85	*86*	87	*88*	89	*90*
91	*92*	93	*94*	95	*96*	97	*98*	99	*100*

4. Repeat steps 2-4, unless there are no more unmarked numbers.

After finishing our list, we have

	$\boxed{2}$	$\boxed{3}$	*4*	$\boxed{5}$	*6*	$\boxed{7}$	*8*	*9*	*10*
$\boxed{11}$	*12*	$\boxed{13}$	*14*	*15*	*16*	$\boxed{17}$	*18*	$\boxed{19}$	*20*
21	*22*	$\boxed{23}$	*24*	*25*	*26*	*27*	*28*	$\boxed{29}$	*30*
$\boxed{31}$	*32*	*33*	*34*	*35*	*36*	$\boxed{37}$	*38*	*39*	*40*
$\boxed{41}$	*42*	$\boxed{43}$	*44*	*45*	*46*	$\boxed{47}$	*48*	*49*	*50*
51	*52*	$\boxed{53}$	*54*	*55*	*56*	*57*	*58*	$\boxed{59}$	*60*
$\boxed{61}$	*62*	*63*	*64*	*65*	*66*	$\boxed{67}$	*68*	*69*	*70*
$\boxed{71}$	*72*	$\boxed{73}$	*74*	*75*	*76*	*77*	*78*	$\boxed{79}$	*80*
81	*82*	$\boxed{83}$	*84*	*85*	*86*	*87*	*88*	$\boxed{89}$	*90*
91	*92*	*93*	*94*	*95*	*96*	$\boxed{97}$	*98*	*99*	*100*

The boxed items are primes; the italicized items are composites.

4.2 The number of primes

The following proof is due to Euclid, another ancient mathematician. It is a classic example of proof by contradiction.

Let us suppose that there is a finite number of primes. Multiply them all together to get a huge - but still finite - integer n. Note that n must be larger than all the primes. Now let us consider the factors of $n+1$. Then, since $n+1 > n >$ all primes, $n+1$ must be composite. Hence there exists an prime p such that $\frac{n+1}{p} \in \mathbb{Z}$. But note that $\frac{n+1}{p} = \frac{n}{p} + \frac{1}{p}$. Since n is defined as the product of all primes, p must divide it - hence, $\frac{n}{p} \in \mathbb{Z}$, so, since $\frac{1}{p}$ is clearly not an integer, $\frac{n+1}{p}$ is not an integer; hence, p does *not* divide $n + 1$. But p was defined to be a factor of $n + 1$! By this contradiction, we conclude that our assumption (that there is a finite number of primes) is wrong; hence, there is an infinite number of primes.

QED/VIM

4.3 Primality testing

The most obvious way to determine whether a number is prime is to divide it by all primes less than it; however, there is a better way. Since $\frac{n}{\sqrt{n}} = \sqrt{n}$, we only need to divide by primes up to $\sqrt{n}$.

There are many, many methods of determining primality that work a lot faster than this - provided that the Riemann Hypothesis is true. However, that is a discussion requiring some very advanced techniques that we cannot include here.

4.4 Prime factorization

The prime factorization of a number is the product of primes that yields the number. The fact that each number has a unique prime factorization (aside from rearrangements of factors) is called the *fundamental theorem of arithmetic.* When prime factors are repeated, we usually combine them as a prime to a power, and we also arrange these terms so that the bases increase from left to right. Hence, we would usually write a factorization as

$$p_1^{a_1} p_2^{a_2} \dots p_n^{a_n} \tag{2}$$

with $p_1 < p_2 < \dots < p_n$. For example, we would write the prime factorization of 2296458000 as $2^4\ 3^3\ 5^3\ 23\ 43^2$.

5 LCM

The *l*east *c*ommon *m*ultiple of a pair of numbers. We usually write it as $LCM(x, y)$.

Let the numbers we are concerned with be a and b. The most obvious way to compute $LCM(a, b)$ is to multiply a by successively increasing integers, starting with 1, and stopping when we have a number divisible by b. But there is a better way to do this. Let the numbers we are concerned with be a and b. Find the largest power of each prime factor of a that still divides a, find the corresponding powers for b, and take the larger of the two powers. A more rigorous description of this method follows:

5.1 Calculation

1. Find the prime factorization of each number. Express one as $2^{a_1}3^{a_2}5^{a_3}$... and the other as $2^{b_1}3^{b_2}5^{b_3}$....

2. For all i, let $c_i = max(a_i, b_i)$.

3. The least common multiple is $2^{c_1}3^{c_2}5^{c_3}$....

6 GCD

The *g*reatest *c*ommon *d*ivisor of two numbers. We usually write this as $GCD(x, y)$. There are two main methods to find this. The first is rather similar to our method of finding the LCM; the second is surprisingly elegant.

6.1 Computation via factorization

1. Find the prime factorization of each number. Express one as $2^{a_1}3^{a_2}5^{a_3}$... and the other as $2^{b_1}3^{b_2}5^{b_3}$....

2. For all i, let $c_i = min(a_i, b_i)$.

3. The greatest common divisor is $2^{c_1}3^{c_2}5^{c_3}$....

6.2 Computation via the Euclidean Algorithm

We often want to find the GCD of numbers that would be very tedious to factorize. Fortunately, there is another method we can use to compute the GCD. The Euclidean algorithm is based on the fact that $GCD(a,b) = GCD(b, a-cb)$, and is implemented as follows.

$$a = d_0 b + c_0 \tag{3}$$

$$b = d_1 c_0 + c_1 \tag{4}$$

$$c_0 = d_2 c_1 + c_2 \tag{5}$$

$$c_1 = d_3 c_2 + c_3 \tag{6}$$

$$c_2 = d_4 c_3 + c_4 \tag{7}$$

$$\vdots$$

$$c_{k-2} = d_k c_{k-1} + c_k \tag{8}$$

$$c_{k-1} = d_{k+1} c_k \tag{9}$$

c_k will be the GCD we seek.

An example: compute GCD(920,720).

$$920 = 1 \cdot 720 + 200$$

$$720 = 3 \cdot 200 + 120$$

$$200 = 1 \cdot 120 + 80$$

$$120 = 1 \cdot 80 + 40$$

$$80 = 2 \cdot \boxed{40} + 0$$