NUMBER THEORY

BY THE SPMPS 2013 NUMBER THEORY CLASS

Abstract. This paper presents theorems proven by the Number Theory class of the 2013 Summer Program in Mathematical Problem Solving. An appendix is included with a table giving the number of divisors of various natural numbers. The ideas in this paper were created by Tiffany Baez, Seth Guasp, Janequa Mason, Felix Perez, Vielka Rankin, Agustin Read, Jayden Reaves, Christian Rosado, Thalyia Thompson, and Pamela Vargas. The paper was edited by Ben Blum-Smith.

1. Divisor Counting

Theorem 1. *A number is a square if and only if it has an odd number of factors.*

Proof. If the number is not a square, then the factors all come in pairs, thus there are an even number of them.

If the number is a square, all of the factors are in pairs except the square root. So the total number of factors is odd. □

Theorem 2. 1 *is the only natural number with only one divisor.*

Proof. If $n \neq 1$, then n has at least 2 divisors: 1 and n. □

Theorem 3. 0 *is the only nonnegative integer with infinitely many divisors.*

Proof. First, 0 has infinitely many divisors because every nonnegative integer is a divisor of zero, because for all x, $0 \cdot x = 0$.

Secondly, if $n \neq 0$, then for any $m > n$, m is not a divisor of n. Therefore, all the divisors of n lie between 1 and n. So there cannot be infinitely many. □

2. Squares

Theorem 4. *The differences between consecutive square numbers are consecutive odd numbers. More specifically,*

$$(n+1)^2 - n^2 = n + (n+1) = 2n + 1$$

Proof.

$$\begin{aligned}(n+1)^2 &= (n+1)(n+1)\\ &= n^2+n+n+1\\ &= n^2+2n+1\end{aligned}$$

Therefore,

$$(n+1)^2 - n^2 = (n^2+2n+1) - n^2 = 2n+1$$

□

Since every odd number 3 and up has the form $2n+1$ for some natural number n, this means every odd number 3 and up occurs as a difference of squares.

Here is a consequence of this:

Theorem 5. *There are infinitely many square numbers that are the sum of two other square numbers.*

Proof. Each odd square number will eventually occur as the difference between two consecutive squares because all odd numbers 3 and up occur this way because of theorem 4. In other words, if m is odd and at least 3, then m^2 is odd, so that

$$m^2 = 2n+1$$

for some nonnegative integer n.

But then by the last result, $(n+1)^2 - n^2 = 2n+1 = m^2$, so

$$m^2 + n^2 = (n+1)^2$$

Since this works for any choice of odd $m \geq 3$, this gives us an infinite list of squares $(n+1)^2$ that are sums of two other squares. □

3. Primes

Theorem 6. *n and $n+1$ can both be prime, but only if $n=2$ and $n+1=3$.*

Proof. For any choice of n, one of n or $n+1$ will be even. The only even prime number is 2. Every other even number is composite. So, if $n > 2$, then so is $n+1$, therefore, the even one is composite. □

Theorem 7. *Except for 2 and 3, all prime numbers are 1 or 5 mod 6.*

Proof. If a number is divisible by 6, it is composite; thus no prime number is 0 mod 6. If a number is 2 more than a multiple of 6, it is even, because all multiples of 6 are even. The only even prime is 2. Thus a prime number cannot be 2 mod 6 unless it is actually equal to 2. Similarly, if a number is 3 more than a multiple of 6, it is a multiple of 3, since all multiples of 6 are multiples of 3. Since 3 is the only multiple of 3 that is prime, this means that a prime number cannot be 3 mod 6 unless it is actually equal to 3. Finally, if a number is 4 mod 6, then it is even for the same reason that any number that is 2 mod 6 is even, and therefore it cannot be prime.

Thus no prime number other than 2 or 3 can be equal to 0, 2, 3, or 4 mod 6. It must be that all the prime numbers except 2 and 3 are 1 or 5 mod 6. □

Theorem 8. *For any natural number $n \neq 0$, no number bigger than $n/2$ can be a factor of n except n itself.*

Proof. Suppose $x \geq n/2$ but $x \neq n$. Then $x \cdot 2 > n$ because $x > n/2$. And $x \cdot 1 \neq n$ because $x \neq n$. And $x \cdot$ anything bigger than $2 > x \cdot 2 > n$. Also, $x \cdot 0 \neq n$ because $n \neq 0$. Therefore there is no number that times x is n. Therefore x is not a factor of n. □

Corollary 1 (First primality test)**.** *To check if a number n is prime, divide n by every natural number > 1 and $\leq n/2$. If each division gives a non-whole answer, then n is prime.*

Proof. Theorem 8 shows that no natural number $> n/2$ can be a divisor of n except n itself. If all the divisions in the test give a non-whole answer, this also shows that no natural number from 2 to $n/2$ can be a divisor. This implies that the only divisors of n can be 1 and n. Therefore n is prime. □

Theorem 9. *127 is prime.*

Proof. If it were not prime, then it would be a product

$$127 = a \cdot b$$

with $a, b > 1$. We checked that a, b cannot be 2 through 12 using divisibility rules. Thus the smallest number $a \cdot b$ could be is $13 \cdot 13$. But this is > 127. So it is impossible for $127 = a \cdot b$ with $a, b > 1$. Therefore 127 is prime. □

Theorem 10. *947 is prime.*

Proof. As in the proof of theorem 9, if 947 were composite, it would be a product

$$947 = a \cdot b$$

with $a, b > 1$. We checked divisibility of 947 by every prime number less than 30. This rules out the possibility that a or b could be any prime number less than 30. Also, neither a nor b could be a composite number less than 30, because if 947 were divisible by a composite number less than 30 then it would also be divisible by the prime factors of that number which are also less than 30 and we have ruled this out.

This shows that 947 is not divisible by any number from 2 to 30. Thus the smallest possible proper factorization $a \cdot b$ that is possible is $31 \cdot 31$. But this is 961, which is bigger than 947. So no proper factorization is possible. Thus 947 is prime. □

The method used in these proofs can be generalized to create a better primality test than the one described in corollary 1.

Theorem 11 (Existence of factorizations)**.** *Every composite number can be expressed as a product of two or more prime numbers.*

Proof. If n is composite, it can be expressed as a product of two or more prime numbers using a factor tree. This works because of the following reason:

If n is not zero, its factor tree will end. If the factor tree didn't end, it would contain an infinite sequence of divisors, each smaller than the last. Therefore n would have infinitely many divisors. But the only nonnegative number with infinitely many divisors is zero, by theorem 3. So if n is not zero, the factor tree must end. □

Theorem 12 (Infinitude of the primes)**.** *There are infinitely many prime numbers.*

Proof. Start with a finite list of prime numbers

$$2, 3, 5, 7, \ldots, P$$

where P is some big prime.

Consider the number

$$N = 2 \cdot 3 \cdot 5 \cdot 7 \cdot \ldots \cdot P + 1$$

N is not divisible by any of the primes $2, 3, \ldots, P$ on the list, because $2 \cdot 3 \cdot \ldots \cdot P$ is divisible by all of them, and N is 1 greater than this; therefore N would have a remainder of 1 when divided by any prime on the list.

If N is prime, it can be added to the list. If N is not prime, then because of theorem 11, it can be factored into a product of primes. Because N is not divisible by any prime on the list, it must be that its factors are *not* on the list. Then we can add these numbers to the list.

This process yields a longer list of primes. We can repeat the process, yielding a list that is still longer. Since at each step, the list will be made longer, it follows that the primes do not end. □

4. Appendix

This is a table listing the number of divisors of various natural numbers:

1 divisor	2 divisors	3 divisors	4 divisors	5 divisors	6 divisors	7 divisors
1	109	9	93	16	92	64
	97	25	82		18	
	67	4	77		28	
	83	49	62		44	
	61		6		20	
	11		51		12	
	41		21		45	
	3		39		50	
	13		8		63	
	23		14		32	
	43		38		52	
	19		33		68	
	29		34		98	
	59		10		99	
	5		15		75	
	2		35			
	7		22			
	17		55			
	37		85			
	47		58			
	53		27			
	79		57			
	89		87			
	31		26			
			69			
			74			
			94			
			65			
			46			
			95			

8 divisors	9 divisors	10 divisors	11 divisors	12 divisors	∞ divisors
30	36	48	1024	60	0
24		80		84	
54				72	
42				90	
40					
78					
56					
70					
88					
104					