2. Prime Numbers

You probably know that the numbers 2, 3, 5, 7, 11, 13 and 17 are prime numbers. We give a precise definition of the notion of prime number below.

Definition 2.1: A number $p \in \mathbb{N}$ is a prime number if and only if $p \geq 2$ and the only natural numbers which divide *p* are 1 and *p*.

The prime numbers between 1 and 100 are given by 2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, 59, 61, 67, 71, 73, 79, 83, 89 and 97.

Prime numbers and their properties were first studied by the ancient Greek mathematicians of Pythagoras's school from 500 BC to 300 BC. Book IX of Euclid's *Elements* (300 BC) contains a proof that there are infinitely many prime numbers. Euclid also proved the Fundamental Theorem of Arithmetic; namely that every natural number can be written in a unique way as a product of primes. There are a multitude of mathematical results related to prime numbers. Interestingly though, there is no formula for easily determining whether a natural number is a prime number, and it is very difficult to determine (even with a high powered computer) whether a very large natural number is prime. The largest known prime was found by the Great Internet Mersenne Prime Search in November 2003 (and perhaps not the most recent by the time you read these notes) has 6,320,430 decimal digits. **That's HUGE!** In fact, it could take over 1,500 pages to write this prime number in a 12 point font!

Definition 2.2: Let $n \geq 2$ be a natural number. A prime factorization of *n* has the form

$$n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}$$

where $p_1, p_2, ..., p_k$ are prime numbers and $\alpha_1, \alpha_2, ..., \alpha_k \in \mathbb{N}$.

Theorem 2.3: Every natural number $n \geq 2$ has a unique prime factorization.

Proof: If *n* is prime, there is nothing to prove. So, suppose *n* is not prime. Then, there exists an integer *k* such that $1 < k < n$ and *k* divides *n*. Pick the smallest such integer and call it p_1. If p_1 were not prime, then it would have a divisor *q* such that $1 < q < p_1$. But, *q* divides p_1 implies that *q* divides *n*, which contradicts to the minimality of p_1. Thus, p_1 is prime. Write $n = p_1 m_1$. If m_1 is prime, we have the desired representation. Otherwise, with the same argument, we obtain p_2 such that $m_1 = p_2 m_2$, and this implies that $n = p_1 p_2 m_2$. The decreasing sequence $n > m_1 > m_2 > ... > 1$ can not continue indefinitely, so at some point m_{k-1} is a prime; call it p_k. Then $n = p_1 p_2 ... p_k$ is the prime factorization of *n*.

To show uniqueness, assume that we have two prime factorizations.

$$n = p_1 p_2 ... p_r = q_1 q_2 ... q_s$$

We can assume that $r \le s$, and that our primes are written in an increasing way;

$$p_1 \le p_2 \le ... \le p_r \text{ and } q_1 \le q_2 \le ... \le q_s .$$

Since p_1 divides $q_1 q_2 ... q_s$, and the q_i are prime, we must have $p_1 = q_k$ for some k, but then $p_1 \ge q_1$. The same reasoning gives $q_1 \ge p_1$, so $p_1 = q_1$. Cancel this common factor to get $p_2 p_3 ... p_r = q_2 q_3 ... q_s$. Continuing in this way, we can divide by all p_i and get $1 = q_{r+1} q_{r+2} ... q_s$. But the q_i were assumed to be greater than or equal to 1, so they must be equal to 1. Then $r = s$ and $p_i = q_i$ for all i, making the factorizations equal. ■

The following result can help determine whether a natural number is prime, and lessen the pain of finding a prime factorization.

Theorem 2.4: Let $n \ge 2$ be a natural number and suppose $k \in \mathbb{N}$ so that $k^2 > n$. n is a prime number if and only if no prime number less than k divides n.

Proof: ($\Rightarrow$) Suppose n is prime. Then by definition of prime numbers, its only divisors are 1 and n. Thus, n is not divisible by any of the prime numbers less than k (note that n itself is not one of those numbers since $k^2 > n$).

($\Leftarrow$) Suppose none of the prime numbers less than k divides n. Then, any natural number (except 1 of course!!!) less than or equal to k does not divide n (since any such natural number is either a prime number less than k or a product of prime numbers which are less than k). Let p be a natural number which is bigger than k ($p \ne n$). Suppose p divides n. There exists a natural number q such that $n = q \cdot p$. Since $k^2 > n$, we have; $q \cdot p < k^2$. We know that $p > k$, so q must be smaller than k. Hence, q is a natural number that divides a and it is smaller than k. But this is a contradiction to our hypotheses since q is either a prime number less than k or is a product of prime numbers which are less than k. Hence, n does not have any divisors other than 1 and itself; n is prime. ■

Example 2.5: Show that the numbers 2, 3, 5 and 7 can be used to determine all of the prime numbers smaller than 100.

Solution: Let $n \in \mathbb{N}$ with $n < 100$. Notice that $10^2 = 100 > n$, and the prime numbers less than 10 are 2, 3, 5 and 7. So, Theorem 2.4 tells us that n is a prime number if and only if the numbers 2, 3, 5 and 7 do not divide n.

Remark 2.6: The example above can be used to identify the prime numbers less than 100. We create a table of natural numbers between 2 and 100 and shade the cells of any number other than 2, 3, 5 and 7 that is a multiple of one of these numbers.

	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

The multiples of 2 (other than 2) are shaded red, the remaining multiples of 3 (other than 3) are shaded blue, the remaining multiples of 5 (other than 5) are shaded yellow, and the remaining multiples of 7 (other than 7) are shaded green. The numbers whose cells are not shaded are prime numbers!

Remark: The process shown above is referred to as the Sieve of Eratosthenes. An interactive website for the Sieve of Eratosthenes is listed below.

http://matti.usu.edu/nlvm/nav/frames_asid_158_g_2_t_1.html?open=instructions

Example 2.7: Show that 421 is a prime number.

Solution: Notice that $21^2 = 441 > 421$. Consequently, 421 is a prime number if none of 2, 3, 5, 7, 11, 13, 17 and 19 divide 421. We can see that 421 is not even, so 2 does not divide 421. The digits of 421 do not sum to a multiple of 3, so 3 does not divide 421. The last digit of 421 is not 0 or 5, so 5 does not divide 421. The remaining checks require a little more effort, but we can verify that 7, 11, 13, 17 and 19 do not divide 421. Therefore, 421 is a prime number.

Example 2.8: Give the prime factorization of the number 12426.

Solution: The number 12426 is an even number, so it is divisible by 2. Also, the sum of the digits is 15, which is divisible by 3. So 12426 is divisible by 3. A simple computation shows

$$12426 = (2)(3)2071$$

The exercises above can be used to show that 2071 is not divisible by 2, 3 or 5. A manual check shows that 2071 is also not divisible by 7, 11, 13 or 17, but it is divisible by 19, and $2071 = (19)(109)$. Therefore,

$$12426 = (2)(3)2071 = (2)(3)(19)(109)$$

Now, $11^2 > 109$, so from Theorem 2.4, 109 is prime if 2, 3, 5, and 7 are not divisors of 109. The criteria from earlier exercises shows that 2, 3 and 5 are not divisors of 109. Long division shows that 7 is also not a divisor. As a result, 109 is prime. Therefore, the prime factorization of 12426 is given by

$$12426 = (2)(3)(19)(109)$$

Example 2.9: Give the prime factorization of 2303028.

Solution: 2303028 is a multiple of 4 since its last two digits are divisible by 4. Also,

$$2303028 = 4(575757) = (2)^2(575757)$$

Notice that the digits of 575757 sum to 36, and 36 is a multiple of 9. As a result, 575757 is a multiple of 9. In fact,

$$575757 = 9(63973) = (3)^2(63973)$$

So,

$$2303028 = 4(575757) = (2)^2(575757) = (2)^2(3)^2(63973)$$

We can see that 2, 3 and 5 do not divide 63973. However, the next prime, 7, divides this number, and $63973 = 7(9139)$. This gives

$$2303028 = (2)^2(3)^2(7)(9139)$$

Neither 7 nor 11 divide 9139, but 13 divides this number, and $9139 = 13(703)$. Combining this information gives

$$2303028 = (2)^2(3)^2(7)(13)(703)$$

13 and 17 do not divide 703, but 19 divides this number, and $703 = 19(37)$. Since 37 is prime, we have the prime factorization

$$2303028 = (2)^2(3)^2(7)(13)(19)(37)$$

Remark 2.10: The example above illustrates that it can be very painful to find the prime factorization of a large natural number. It can even be difficult for computers to find the prime factorization of extremely large natural numbers.

Theorem 2.11: Let $n \in \mathbb{N}$ with $n \geq 2$. Suppose $p_1, p_2, ..., p_k$ are distinct prime numbers and $\alpha_1, \alpha_2, ..., \alpha_k \in \mathbb{N}$ so that

$$n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}$$

is the prime factorization of n. Then n has $(\alpha_1 + 1)(\alpha_2 + 1)\cdots(\alpha_k + 1)$ factors. Furthermore, the factors are given all of the values

$$p_1^{\beta_1} p_2^{\beta_2} \cdots p_k^{\beta_k}$$

with $\beta_i \in \{0, 1, ...\}$ and $0 \leq \beta_i \leq \alpha_i$ for each $i = 1, ..., k$.

Proof: This is simply a matter of counting. Notice that the prime factors of any factor of n must be contained in the set $\{p_1, p_2, ..., p_k\}$. Furthermore, The exponents of any of these primes can not exceed the exponents $\alpha_1, \alpha_2, ..., \alpha_k$ for n. As a result, for the prime p_1, the factor can have any one of $\alpha_1 + 1$ exponents

(including 0, 1, ..., α_1), for the prime p_2, the factor can have any one of α_2+1 exponents (including 0, 1, ..., α_2), etc. up to p_k. Taking all of these exponents into account, we have $(\alpha_1+1)(\alpha_2+1)\cdots(\alpha_k+1)$ possible factors of *n*, having the form given in the statement of the theorem above. ■

Example 2.12: The prime factorization of the number 180 is $(2)^2(3)^2(5)$. Consequently, 180 has $(2+1)(2+1)(1+1)=18$ factors. Each factor can be written in the form $(2)^a(3)^b(5)^c$ where $a\in\{0,1,2\}$, $b\in\{0,1,2\}$ and $c\in\{0,1\}$. The 18 different factors can be created using the table below.

$a\in\{0,1,2\}$	$b\in\{0,1,2\}$	$c\in\{0,1\}$	$(2)^a(3)^b(5)^c$
0	0	0	1
0	0	1	5
0	1	0	3
0	1	1	15
0	2	0	9
0	2	1	45
1	0	0	2
1	0	1	10
1	1	0	6
1	1	1	30
1	2	0	18
1	2	1	90
2	0	0	4
2	0	1	20
2	1	0	12
2	1	1	60
2	2	0	36
2	2	1	180

Theorem 2.13: There are infinitely many prime numbers.

Proof: Assume for contradiction that there are a finite number of prime numbers. Let's call them $p_1, p_2, p_3, ..., p_N$. Consider the number

$$p=(p_1\cdot p_2\cdot p_3\cdot\ldots\cdot p_N)+1$$

Notice that this number is larger than all of the primes listed above. Also, none of the primes listed above are divisors of this number. As a result, $p=(p_1\cdot p_2\cdot p_3\cdot\ldots\cdot p_N)+1$ must be a prime number, and we have a contradiction. ■

Exercises – Use Hand Calculations On The Exercises Below.

1. Use the exercises at the end of the previous section and the list of primes

at the beginning of this section to give the prime factorization of 42042.

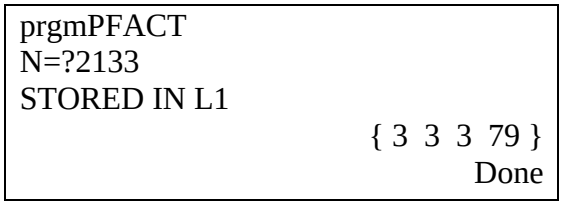
2. Use the exercises at the end of the previous section and the list of primes at the beginning of this section to give the prime factorization of 109460.
3. Use Theorem 2.4 to show that 359 is prime. (Hint: $19^2 > 359$)
4. Use Theorem 2.4 to show that 887 is prime. (Hint: $30^2 > 887$)
5. Create a table of natural numbers between 2 and 200. Explain how the multiples of 2, 3, 5, 7, 11 and 13 (other than 2, 3, 5, 7, 11 and 13) can be used to determine the prime numbers in this table. Use your process to determine the prime numbers less than 200.
6. Use Theorem 2.11 to determine the number of factors of 260. Then use a table (like the one in Example 2.12) to list all of the factors of 780.
7. Use Theorem 2.11 to determine the number of factors of 1260.
8. Let $n \in \mathbb{N}$ with $n \geq 2$. Show that n has an odd number of factors if and only if $n = q^2$ for some natural number q.
9. Two natural numbers are said to be twin primes if they are both prime numbers and they differ by 2. For example, 5 and 7 are twin primes. 17 and 19 are twin primes. Use the table created in the exercise above to list all of the twin primes less than 200.

TI-83 Programs For Testing Primes and Finding Prime Factors

The TI-83 program PCHECK determines whether a natural number is a prime number. The program PFACT gives the prime factors of a natural number.

PCHECK	PFACT
: Prompt N	**: ClrList L1**
: iPart(√ (N)) → M	**: Prompt N**
: For(I,2,M)	**: iPart(√ (N)) → M**
: If iPart(N/I) = N/I	**: 2 → I**
: Then	**: 1 → J**
: Goto B	**: While I ≤ M**
: End	**: While N/I ≤ iPart(N/I)**
: End	**: I → L1(J)**
: Disp "PRIME"	**: J+1 → J**
: Goto C	**: N/I → N**
: Lbl B	**: End**
: Disp "NOT PRIME"	**: I+1 → I**
: Disp I	**: End**
: Disp "IS A DIVISOR"	**: If N > 1**
: Lbl C	**: Then**
	: N → L1(J)
	: End
	: Disp "STORED IN L1"
	: Disp L1

Enter these programs into your calculator. The program PCHECK will prompt you for a number. After you input the value it will tell you whether the number is prime or not. If it is not prime, it will give you a prime divisor of the number. The program PFACT will prompt you for a number, and return a list of prime factors of the number. This list is stored in L_1 for later reference. The screen shot below shows the result of running the PFACT program with an input of 2133.



The output tells us that the prime factorization of 2133 is given by $(3)^3(79)$.

Remark 2.12: PFACT can take considerable time to run if N is large. For example, PFACT takes nearly 30 seconds to give the prime factorization of N = 2303028. Also, it will be necessary to view the list L_1 (using the scrolling arrows) to view the prime factors since the list exceeds the width of the calculator screen.