Chapter 5. Some Topics Involving Prime Numbers

The RSA Scheme

5.1 Definition: Cryptography is the study of secret codes. When we convert a message from a normal language, say English, to a secret code, we say that we **encrypt** (or **encipher**) the message, and the coded word is called the **ciphertext**. When we convert the ciphertext back into normal language, we say that we **decipher** (or **decrypt**) the ciphertext to obtain the original message.

5.2 Example: One of the simplest encryption methods is a **Caesar cipher**. Suppose Alice wants to send a secret message to Bob using a Caesar cipher. Alice and Bob agree in advance on a number n between 1 and 25. Alice encrypts the message by replacing each letter in the message by the letter which follows it by n positions (modulo 26) in the English alphabet. For example, if $n = 4$ then the letter P would be replaced by the letter T (which follows P by 4 positions), and the message PONY would be replaced by the ciphertext TSRC. Bob can easily decrypt the ciphertext by replacing each letter by the letter which precedes it by n positions.

5.3 Example: A slightly more secure encryption method is a **substitution cipher**. Suppose that Alice wants to send a secret message to Bob using a substitution cipher. Alice and Bob agree in advance on a permutation p of the letters of the English alphabet. Alice enciphers the message by replacing each letter by the letter which corresponds to it under the permutation p. For example, if the permutation p is given as follows

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
V	G	S	C	F	U	Q	L	A	P	I	D	X	N	W	T	H	Y	O	J	K	Z	B	E	R	M

then the letter H would be replaced by the letter L and the message HORSE would be replaced by the ciphertext LWYOF.

5.4 Definition: A far more secure encryption system, which is commonly used by modern computers, is the **RSA scheme**. The letters R, S and A stand for Rivest, Shamir and Adleman, who first described this encryption system. The RSA scheme is a **public key** encryption system, which means that when a person, say Alice, wishes to receive a secret message, she makes her encryption rules publicly known so that anyone can encipher a message and send it to Alice and yet, although everyone knows the encryption rules, only Alice knows the decryption rules and can decipher the ciphertext.

Suppose that Alice wishes to receive a secret message using the RSA scheme. Alice chooses two large prime numbers p and q (in practice, p and q would have over 100 decimal digits) and calculates $n = pq$ and $\varphi = \varphi(n) = (p-1)(q-1)$. Then Alice chooses a positive integer $e < \varphi$ with $\gcd(e, \varphi) = 1$ and calculates $d = e^{-1} \mod \varphi$. The number e is called the **encryption key** and the number d is called the **decryption key**. Then Alice makes the numbers n and e publicly known. Suppose that Bob wishes to send a message to Alice. Bob converts his message to a positive integer m with $m < n$ (if his message is too long then he breaks it into shorter messages). Bob calculates the ciphertext $c = m^e \mod n$ which he sends to Alice. Note that since $ed = 1 \mod \varphi$, we have $c^d = (m^e)^d = m^{ed} = m^1 = m \mod n$ by the Euler Fermat Theorem, and so Alice can recover the original message m by calculating $m = c^d \mod n$.

5.5 Note: Alice can save some time if, instead of calculating $\varphi = (p-1)(q-1)$ and $d = e^{-1} \bmod \varphi$, she instead calculates $\psi = \text{lcm}(p-1, q-1)$ and $d = e^{-1} \bmod \psi$. Verify that when $c = m^e \bmod n$ we have $c^d = (c^e)^d = c^{ed} = c^1 = m \bmod n$.

5.6 Note: The reason that the RSA scheme is practical and secure is that there do exist efficient (polynomial time) algorithms which can be used to find p, q, n, φ, e and d and to calculate $c = m^e \mod n$ and $m = c^d \mod n$, but there is no known efficient algorithm which can be used to determine m from n, e and c. In particular, there do exist efficient algorithms which can be used to determine whether a given positive integer n is prime, but there is no known efficient algorithm which can determine a prime factor of n in the case that n is composite.

There do, of course, exist inefficient algorithms which can determine a prime factor of n. For example, we can use the Sieve of Eratosthenes to list all primes p with $1 < p \leq \sqrt{n}$ and then test each such prime p to determine whether it is a factor of n. But when the prime factors of n are over a hundred digits long, this algorithm is too slow (if a computer could list 10^{10} prime numbers each second then it would take about 10^{80} years to list all the prime numbers p with $p < 10^{100}$).

5.7 Example: The calculation of $d = e^{-1} \mod \varphi$ can be performed using the Euclidean Algorithm, which is efficient.

5.8 Example: When n, e and m are all large, we can calculate $c = m^e \mod n$ efficiently as follows. Express e in base 2, say $e = \sum_{i=1}^{\ell} 2^{k_i}$ with $0 \leq k_1 < k_2 < k_3 < \cdots$, calculate the residues $m^1, m^2, m^4, m^8, \cdots, m^{2^{k_\ell}} \mod n$, then calculate $c = m^e = \prod_{i=1}^{\ell} m^{2^{k_i}} \mod n$. This algorithm is known as the **Square and Multiply Algorithm**.

5.9 Example: Alice wishes to receive a message. She chooses $p = 13$ and $q = 17$ and calculates $n = pq = 221$. She also chooses $e = 35$ and makes the numbers n and e public. Bob wishes to secretly send Alice the letter T. Bob converts the letter T to the number $m = 20$ (since T is the 20^{th} letter in the English alphabet) and sends the cyphertext $c = m^e \bmod n$. As an exercise, calculate $c = m^e \bmod n$ and calculate $\psi = \text{lcm}(p-1, q-1)$ and $d = e^{-1} \bmod \psi$, then directly calculate $c^d \bmod n$ to verify that $c^d = m \bmod n$.

Primality Tests and Carmichael Numbers

5.10 Definition: Let us describe a simple test for primality which is called the **Fermat Primality Test**. Suppose that we are given an integer $n > 2$. Choose an integer a with $1 < a < n$. By Fermat's Little Theorem, if n is prime then we must have $\gcd(a, n) = 1$ and $a^{n-1} = 1 \mod n$, so we use the Square and Multiply Algorithm to calculate $a^{n-1} \mod n$. If $a^{n-1} \neq 1 \bmod n$ then we can conclude that n is composite while if $a^{n-1} = 1 \mod n$ then we can conclude that n is probably prime.

5.11 Example: Unfortunately, given $n, a \in \mathbb{Z}^+$ with $1 < a < n$, if $a^{n-1} = 1 \bmod n$ then it does not necessarily follow that n is prime. For example, verify that $2^{340} = 1 \bmod 341$ but $341 = 11 \cdot 31$. As another example, verify that $3^{90} = 1 \bmod 91$ but $91 = 7 \cdot 13$.

5.12 Definition: Let $n, a \in \mathbb{Z}^+$ with n composite and $1 < a < n$. If $a^{n-1} \neq 1 \mod n$ then we say that a is a **Fermat witness** for the compositeness of n. If $a^{n-1} = 1 \mod n$ then we say that a is a **Fermat liar** and that n is a **Fermat pseudoprime** in the base a.

5.13 Note: We can improve the reliability of the above test simply by repeating it. Given $n \in \mathbb{Z}^+$, we choose a finite set S of integers a with $1 < a < n$. For each $a \in S$ we calculate $a^{n-1} \mod n$. If we find some $a \in S$ such that $a^{n-1} \neq 1 \mod n$ then we know that n is composite. If we find that for every $a \in S$ we have $a^{n-1} = 1 \mod n$ then we can conclude that n is probably prime.

5.14 Example: Unfortunately, if if $a^{n-1} = 1 \mod n$ for every a with $1 < a < n$ and $\gcd(a, n) = 1$ then it does not necessarily follow that n is prime. For example, show that when $n = 3 \cdot 11 \cdot 17 = 561$ we have $a^{n-1} = 1 \mod n$ for all $a \in \mathbb{Z}$ with $\gcd(a, n) = 1$.

5.15 Definition: For $n \in \mathbb{Z}^+$ we say that n is a **Carmichael number** when n is composite and $a^{n-1} = 1 \mod n$ for every $a \in \mathbb{Z}$ with $\gcd(a, n) = 1$.

5.16 Theorem: *(Carmichael Numbers) Let $n \in \mathbb{Z}^+$. Then n is a Carmichael number if and only if $n = p_1 p_2 \cdots p_\ell$ for some $\ell \geq 3$ and some distinct odd prime numbers $p_1, p_2, \cdots, p_\ell$ such that $(p_i - 1)\big|(n-1)$ for all indices i.*

Proof: Suppose that $n = p_1 p_2 \cdots p_\ell$ where $\ell \geq 2$ and the p_i are distinct primes with $(p_i - 1)\big|(n-1)$. Note that n is composite since $\ell \geq 2$. Let $a \in \mathbb{Z}^+$ with $\gcd(a, n) = 1$. Fix an index i. Since $\gcd(a, n) = 1$ we have $p_i \not| \, a$ and so $a^{p_i - 1} = 1 \mod p_i$ by Fermat's Little Theorem. Since $a^{p_i - 1} = 1 \mod p_i$ and $(p_i - 1)\big|(n-1)$, we also have $a^{n-1} = 1 \mod p_i$. Since $a^{n-1} = 1 \mod p_i$ for every index i, it follows from the Chinese Remainder Theorem that $a^{n-1} = 1 \mod n$. Thus n is a Carmichael number.

Suppose that n is a Carmichael number, say $n = \prod {p_i}^{k_i}$ where $p_1, \cdots, p_\ell$ are distinct primes and $k_1, \cdots, k_\ell \in \mathbb{Z}^+$. Choose $a \in U_n$ such that $\operatorname{ord}_n(a) = \lambda(n)$, where $\lambda(n)$ is the universal exponent $\lambda(n) = \operatorname{lcm}\big(\lambda({p_1}^{k_1}), \cdots, \lambda({p_\ell}^{k_\ell})\big)$. Since n is a Carmichael number, we have $a^{n-1} = 1 \in U_n$ and so $n-1$ is a multiple of $\operatorname{ord}_n(a) = \lambda(n)$, that is $\lambda(n)\big|(n-1)$. Recall that $\lambda(2^2) = 2$ and $\lambda(2^k) = 2^{k-2}$ for $k \geq 3$ and $\lambda(p^k) = p^{k-1}(p-1)$ for odd primes p, and so when $k \geq 2$ we have $p\big|\lambda(p^k)$ for all primes p. If we had $k_i \geq 2$ for some i then we would have $p_i\big|\lambda(n)$ and hence, since $\lambda(n)\big|(n-1)$, we would have $p_i\big|(n-1)$, but this is not possible since $p_i\big|n$. Thus we must have $k_i = 1$ for all i, and so $n = p_1 p_2 \cdots p_\ell$. Since n is composite, we must have $\ell \geq 2$. Since $n-1$ is a multiple of $\lambda(n) = \operatorname{lcm}\big(\lambda(p_1), \cdots, \lambda(p_\ell)\big) = \operatorname{lcm}(p_1 - 1, \cdots, p_\ell - 1\big)$ we have $(p_i - 1)\big|(n-1)$ for all i.

To finish the proof we need to show that when $n = p_1 p_2 \cdots p_\ell$ where $\ell \geq 2$ and $p_1, \cdots, p_\ell$ are distinct primes with $(p_i - 1)\big|(n-1)$ for all i, we must have $\ell \geq 3$ and n must be odd. Since $l \geq 2$, at least one of the primes p_i is odd, say p_k is odd. Since $p_k - 1$ is even and $(p_k - 1)\big|(n-1)$, it follows that $(n-1)$ is even and so n is odd.

To show that we must have $\ell \geq 3$, suppose, for a contradiction, that n is a Carmichael number of the form$n = pq$ where p and q are primes with $p < q$ and we have $(p-1)\big|(n-1)$ and $(q-1)\big|(n-1)$. Note that $n - 1 = pq - 1 = p(q-1) + (p-1)$. Since $(q-1)\big|(n-1)$ we have $(q-1)\big|(n-1) - p(q-1)$, that is $(p-1)\big|(p-1)$. But this implies that $q \leq p$ giving the desired contradiction.

5.17 Exercise: Find distinct primes p and q such that $145\,p$ and $145\,q$ are both Carmichael numbers.

5.18 Theorem: *(The Miller-Rabin Test) Let n be an odd prime number and let $a \in \mathbb{Z}$ with $\gcd(a, n) = 1$. Write $n - 1 = 2^s d$ where $s, d \in \mathbb{Z}^+$ with d odd. Then*

$$\text{either } \ a^d = 1 \bmod n \ \text{ or } \ a^{2^r d} = -1 \text{ for some } 0 \le r < s.$$

Proof: First we remark that since n is prime, $\mathbb{Z}_n$ is a field, so for all $x \in \mathbb{Z}_n$ we have

$$x^2 = 1 \Longleftrightarrow x^2 - 1 = 0 \Longleftrightarrow (x-1)(x+1) = 0 \Longleftrightarrow x = \pm 1 .$$

By Fermat's Little Theorem, we have $a^{n-1} = 1 \bmod n$, that is $a^{2^s d} = 1 \bmod n$. By the above remark $\big($using $x = a^{2^{s-1}d}\big)$ it follows that $a^{2^{s-1}d} = \pm 1 \bmod n$. If $a^{2^{s-1}d} \neq -1$ then $a^{2^{s-1}d} = 1$ so, by the above remark again, it follows that $a^{2^{s-2}}d = \pm 1$. Similarly, if $a^{2^{s-1}d} \neq -1$ and $a^{2^{s-2}d} \neq -1$ then $a^{2^{s-2}d} = 1$ and hence $a^{2^{s-3}}d = \pm 1$ and so on. Repeating the above argument we find that if $a^{2^{s-1}d} \neq -1$, $a^{2^{s-2}d} \neq -1$, $\cdots$, $a^{2^2 d} \neq -1$ and $a^{2d} \neq -1$ then $a^{2d} = 1$ and hence $a^d = \pm 1$.

5.19 Definition: Using the above theorem we obtain the following test for primality, called the **Miller-Rabin Primality Test**. Given an odd integer $n \in \mathbb{Z}^+$ write $n - 1 = 2^s d$ and choose an integer a with $1 < a < n$. By the above theorem, if $a^d \neq 1 \bmod n$ and $a^{2^r d} \neq -1 \bmod n$ for all $0 \le r < s$ then we can conclude that n is composite. If, on the other hand, we find that either $a^d = 1 \bmod n$ or $a^{2^r d} = -1 \bmod n$ for some $0 \le r < s$ then we can conclude that n is probably prime.

5.20 Example: Unfortunately, given $n = 1 + 2^s d$ where $s, d \in \mathbb{Z}^+$ with d odd, and given $a \in \mathbb{Z}$ with $1 < a < n$, even if it is true that either $a^d = 1 \bmod n$ or $a^{2^r d} = -1$ for some $0 \le r < s$, it does not necessarily follow that n is prime. For example, verify that when $n = 221 = 13 \cdot 17$ and $a = 174$ we have $s = 2$ and $d = 55$ and $a^{2d} = -1 \bmod n$.

5.21 Definition: Let $n, a \in \mathbb{Z}^+$ where n is an odd composite number and $1 < a < n$. Write $n - 1 = 2^s d$ where $s, d \in \mathbb{Z}^+$ with d odd. If $a^d \neq 1$ and $a^{2^r d} \neq -1$ for all $0 \le r < s$ then we say that a is a **Miller-Rabin witness** (or a **strong witness**) for the compositeness of n. If either $a^d = 1$ or $a^{2^r d} = -1$ for some $0 \le r < s$ then we say that a is a **Rabin-Miller liar** (or a **strong liar**) and that n is a **Rabin-Miller pseudoprime** (or a **strong pseudoprime**) in the base a.

5.22 Note: As with the Fermat primality test, we can make the Miller-Rabin test more reliable simply by repeating it. Given an odd positive integer n, write $n - 1 = 2^s d$ with $s, d \in \mathbb{Z}^+$ and d odd. Choose a finite set S of integers a with $1 < a < n$. For each $a \in S$, calculate $a^{2^r d} \bmod n$ for $0 \le r < s$. If we find some $a \in S$ for which $a^d \neq 1 \bmod n$ and $a^{2^r d} \neq -1$ for all $0 \le r < s$ then we know that n is composite. If, on the other hand, we find that for every $a \in S$, either $a^d = 1 \bmod n$ or $a^{2^r d} = -1 \bmod n$ for some $0 \le r < s$ then we can conclude that n is probably prime.

5.23 Remark: Recall that repeating the Fermat primality test does not make the test become completely reliable because of the existence of Carmichael numbers. The situation is different with the Miller-Rabin primality test. It has been proven that for every composite positive integer n, at least $\frac{3}{4}$ of the numbers a with $1 < a < n$ are strong witnesses for the compositeness of n. It follows that, given an odd composite number n, if we choose m integers a with $1 < a < n$, the probability that none of the numbers a is a strong witness is at most $\frac{1}{4^m}$.

Fermat Primes

5.24 Definition: A **Fermat prime** is a prime number of the form $p = 2^k + 1$ for some $k \in \mathbb{Z}^+$. The first few values of $2^k + 1$ are shown below.

k	1	2	3	4	5	6	7	8	9	10
2^k+1	3	5	9	17	33	65	129	257	513	1025

We see that $2^k + 1$ is prime for $k = 1, 2, 4, 8$ so one might guess (indeed Fermat did guess) that $2^k + 1$ is prime if and only if k is a power of 2.

5.25 Example: Show that if $2^k + 1$ is prime then k must be a power of 2.

Solution: We remark that when r is odd, $x = -1$ is a root of $x^r + 1$, so $x + 1$ is a factor of $x^r + 1$. Suppose that k is not a power of 2. Then we can write $k = 2^n r$ for some $n \geq 0$ and some odd number $r > 1$, and then we have $2^k + 1 = 2^{2^n r} + 1$. By the above remark, $2^{2^n} + 1$ is a factor of $2^{2^n r} + 1 = 2^k + 1$, so $2^k + 1$ is not prime.

5.26 Definition: For $k \in \mathbb{N}$, the number $F_k = 2^{2^k} + 1$ is called the k^{th} **Fermat number**.

5.27 Remark: The Fermat numbers F_k are all prime for $0 \leq k \leq 4$, but these are the only known Fermat primes, and they may well be the only ones.

5.28 Example: Show that if p is a prime factor of $F_k = 2^{2^k} + 1$ then $p = 1 + c\,2^{k+1}$ for some $c \in \mathbb{Z}^+$.

Solution: Suppose that p is a prime factor of $F_k = 2^{2^k} + 1$. Since $p \big| (2^{2^k} + 1)$ we have $2^{2^k} = -1 \bmod p$, hence $2^{2^{k+1}} = \left(2^{2^k}\right)^2 = 1 \bmod p$. Since $2^{2^k} + 1$ is odd, the prime factor p must be odd, so we have $\gcd(2, p) = 1$ so that $2 \in U_p$. In the group of units U_p we have $2^{2^k} = -1$ and $2^{2^{k+1}} = 1$. Since $2^{2^{k+1}} = 1$, it follows from Corollary 3.20 that $\text{ord}_p(2) \big| 2^{k+1}$ so $\text{ord}_p(2) = 2^j$ for some $j \leq k + 1$. If we had $\text{ord}_p(2) = 2^j$ with $j \leq k$ then we would have $2^{2^j} = 1$, hence $2^{2^l} = 1$ for all $l \geq j$, hence in particular $2^{2^k} = 1$, but instead we have $2^{2^k} = -1$. It follows that $\text{ord}_p(2) = 2^{k+1}$. By Fermat's Little Theorem, we have $2^{p-1} = 1$ in U_p, so from Corollary 3.20 we have $\text{ord}_p(2) \big| (p - 1)$, that is $2^{k+1} \big| (p - 1)$, and hence $p = 1 + c\,2^{k+1}$ for some $c \in \mathbb{Z}^+$.

5.29 Example: Show that F_5 is not prime. Indeed, show that 641 is a factor of F_5.

Solution: Note that $641 = 625 + 16 = 5^4 + 2^4$ and $641 = 640 + 1 = 5{\cdot}2^7 + 1$, so we have

$$\begin{aligned} F_5 = 2^{2^5} + 1 = 2^{32} + 1 = 2^4{\cdot}2^{28} + 1 &= (641 - 5^4){\cdot}2^{28} + 1 = 641{\cdot}2^{28} - (5{\cdot}2^7)^4 + 1 \\ &= 641{\cdot}2^{28} - (641 - 1)^4 + 1 = 641{\cdot}2^{28} - 641^4 + 4{\cdot}641^3 - 6{\cdot}641^2 + 4{\cdot}641. \end{aligned}$$

5.30 Example: Show that $F_n = F_0 F_1 F_2 \cdots F_{n-1} + 2$ for all $n \geq 1$.

Solution: We have $F_0 = 3$ and $F_1 = 5$ so that $F_1 = F_0 + 2$. Let $n \geq 1$ and suppose, inductively, that $F_n = F_0 F_1 \cdots F_{n-1} + 2$. Then

$$\begin{aligned} F_{n+1} - 2 = 2^{2^{n+1}} - 1 &= \left(2^{2^n}\right)^2 - 1 = \left(2^{2^n} + 1\right)\left(2^{2^n} - 1\right) \\ &= F_n(F_n - 2) = F_n\left(F_0 F_1 \cdots F_{n-1}\right) = F_0 F_1 \cdots F_n. \end{aligned}$$

5.31 Example: Let $F_k = 2^{2^k} + 1$. Show that if $k \neq l$ then F_k and F_l are coprime.

Solution: Let $k < l$. By the previous example, we have $F_k \big| (F_l - 2)$. Since $F_k \big| (F_l - 2)$ and F_k and F_l are odd, it follows that F_k and F_l are coprime.

Mersenne Primes and Perfect Numbers

5.32 Definition: For $k \in \mathbb{Z}^+$, the number $M_k = 2^k - 1$ is called the k^{th} **Mersenne number**. A **Mersenne prime** is a Mersenne number which is prime. The first few values of M_k are shown below.

k	1	2	3	4	5	6	7	8	9	10
M_k	1	3	7	15	31	63	127	255	511	1023

We note that M_k is prime for $k = 2, 3, 5, 7$ so one might guess that M_k is prime if and only if k is prime.

5.33 Example: Show that for $k \in \mathbb{Z}^+$, if M_k is prime then k must be prime.

Solution: Suppose that k is composite, say $k = rs$ with $1 < r < k$ and $1 < s < k$. Then

$$M_k = 2^k - 1 = 2^{rs} - 1 = (2^r)^s - 1 = \big(2^r - 1\big)\big((2^r)^{s-1} + (2^r)^{s-2} + \cdots + (2^r) + 1\big).$$

Since $r > 1$ and $s > 1$ we have $2^r - 1 > 1$ and $\big((2^r)^{s-1} + (2^r)^{s-2} + \cdots + (2^r) + 1\big) > 1$, and so M_k is composite.

5.34 Example: Show that M_{11} is composite.

Solution: We have $M_{11} = 2^{11} - 1 = 2047$. To determine whether 2047 is prime, we test each prime p with $p \leq \lfloor\sqrt{2047}\rfloor = 45$ to see if it is a factor. Using the Sieve of Eratosthenes, we find that the primes we need to check are $2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43$, and when we test these primes we find that 23 is a factor and that $2047 = 23 \cdot 89$.

5.35 Example: Show that if k and l are coprime then so are M_k and M_l.

Solution: Suppose that M_k and M_l are not coprime. Let $d = \gcd(M_k, M_l)$. Note that d is odd (since M_k and M_l are odd), so 2 is an invertible element in $\mathbb{Z}_d$. Let n be the order of 2 in $\mathbb{Z}_d$ (so n is the smallest positive integer such that $2^n = 1$ in $\mathbb{Z}_d$). Since $d \big| M_k = 2^k - 1$ we have $2^k = 1 \in \mathbb{Z}_d$ and so $n \big| k$. Similarly $n \big| l$ and so $\gcd(k, l) \geq n > 1$.

5.36 Example: Show that for $k, l \in \mathbb{Z}^+$, we have $\gcd(M_k, M_l) = M_{\gcd(k,l)}$ (note that this generalizes the result of the previous example).

Solution: Let $d = \gcd(k, l)$ and let $e = \gcd(M_k, M_l)$. Since $d \big| k$ we can write $k = ds$ for some $s \in \mathbb{Z}$. Then

$$M_k = 2^k - 1 = 2^{ds} - 1 = (2^d - 1)\big((2^d)^{s-1} + (2^d)^{s-2} + \cdots + 1\big)$$

and so $(2^d - 1) \big| M_k$, that is $M_d \big| M_k$. Similarly, since $d \big| l$ we have $M_d \big| M_l$. Since $M_d \big| M_k$ and $M_d \big| M_l$ we have $M_d \big| \gcd(M_k, M_l)$, that is $M_d \big| e$.

Since $d = \gcd(k, l)$ we can choose $x, y \in \mathbb{Z}$ so that $kx + ly = d$. Since $e \big| M_k$, that is $e \big| 2^k - 1$, we have $2^k = 1 \bmod e$, that is $2^k = 1 \in \mathbb{Z}_e$, and hence $2^{kx} = 1 \in \mathbb{Z}_e$. Similarly $2^{ly} = 1 \in \mathbb{Z}_e$ and so $2^d = 2^{kx+ly} = 2^{kx}2^{ly} = 1 \in \mathbb{Z}_e$. Thus $2^d - 1 = 0 \bmod e$ and so $e \big| 2^d - 1$, that is $e \big| M_d$.

5.37 Example: Let p be prime. Show that if q is a prime divisor of $M_p = 2^p - 1$, then $q = 1 \bmod 2p$.

Solution: Let q be a prime divisor of $M_p = 2^p - 1$. Then $2^p = 1 \in U_q$ and so $\text{ord}_q(2) \big| p$. Since $\text{ord}_q(2) \neq 1$ and p is prime, we must have $\text{ord}_q(2) = p$. Recall that $\text{ord}_q(2) \big| |U_q|$, so we have $p \big| q - 1$, that is $q = 1 \bmod p$. Since p and q are both odd, this implies that $q = 1 \bmod 2p$.

5.38 Example: Show that M_{23} is composite.

Solution: We have $M_{23} = 2^{23} - 1 = 8388607$. By Example 5.12, if q is a prime factor of M_{23} then $q = 1 \bmod 46$ so $q = 1, 47, 93, 139, 185, \cdots$. We try $q = 47$ and find that $M_{23} = 47 \cdot 178481$.

5.39 Exercise: Determine the 6 smallest Mersenne primes.

5.40 Definition: A **perfect number** is a positive integer $n \in \mathbb{Z}^+$ which is equal to the sum of its positive proper divisors, that is

$$n = \sum_{d|n\,,\,d\neq n} d = \sigma(n) - n$$

or, equivalently, such that $\sigma(n) = 2n$. The first few Mersenne primes are $M_2 = 3$, $M_3 = 7$ and $M_3 = 31$ and the first few perfect numbers are

$$\begin{aligned} 6 &= 1+2+3 = 2\cdot 3 \\ 28 &= 1+2+4+7+14 = 4\cdot 7 \\ 496 &= 1+2+4+8+16+31+62+124+248 = 16\cdot 31 \end{aligned}$$

One might guess that the perfect numbers are the numbers of the form $n = 2^{p-1}\cdot M_p$ where M_p is a Mersenne prime.

5.41 Remark: It is not known whether or not there exist any odd perfect numbers.

5.42 Example: Show that for $k \in \mathbb{Z}^+$, if M_k is prime then $2^{k-1}M_k$ is perfect.

Solution: Suppose that M_k is prime. Since M_k is prime, the divisors of M_k are 1 and M_k so $\sigma(M_k) = 1 + M_k$. From the formula $\sigma\big(\prod {p_i}^{k_i}\big) = \prod \sigma({p_i}^{k_i})$ it follows that when q is odd we have $\sigma(2^{k-1}q) = \sigma(2^{k-1})\sigma(q)$. Since $M_k = 2^k - 1$, it follows that M_k is odd and so

$$\begin{aligned} \sigma\big(2^{k-1}M_k\big) &= \sigma(2^{k-1})\sigma(M_k) = \big(1+2+2^2+\cdots+2^{k-1}\big)(1+M_k) = (2^k-1)(1+M_k) \\ &= 2^k - 1 + 2^k M_k - M_k = M_k + 2^k M_k - M_k = 2^k M_k = 2\cdot 2^{k-1}M_k \end{aligned}$$

and so $2^{k-1}M_k$ is perfect.

5.43 Example: Show that if $n \in \mathbb{Z}^+$ is even and perfect then $n = 2^{k-1}M_k$ for some Mersenne prime M_k.

Solution: Let n be an even perfect number. Since n is even we can write $n = 2^{k-1}p$ where $k, p \in \mathbb{Z}^+$ with $k \geq 2$ and p odd. Since p is odd we have $\sigma(n) = \sigma(2^{k-1}p) = \sigma(2^{k-1})\sigma(p) = (2^k - 1)\sigma(p)$. Since n is perfect, we also have $\sigma(n) = 2n = 2^k p$ and so

$$(2^k - 1)\sigma(p) = 2^k p. \qquad (1)$$

From (1) we see that $2^k \big| (2^k - 1)\sigma(p)$, and since $\gcd(2^k, 2^k - 1) = 1$ it follows that $2^k \big| \sigma(p)$, say $\sigma(p) = 2^k d$. Put $\sigma(p) = 2^k d$ into (1) to get $(2^k - 1)2^k d = 2^k p$ then divide by 2^k to get

$$(2^k - 1)d = p. \qquad (2)$$

From (2) we see that $d|p$ and $d \neq p$ and $p + d = (2^k - 1)d + d = 2^k d = \sigma(p)$. Since p and d are two distinct divisors of p with $\sigma(p) = p + d$, it follows that p and d are the only divisors of p, so p is prime and $d = 1$. Put $d = 1$ into (2) to get $p = 2^k - 1 = M_k$. Thus $p = M_k$ is a Mersenne prime and $n = 2^{k-1}p = 2^{k-1}M_k$.

Primes in Arithmetic Progression

5.44 Remark: There is a famous theorem, by Dirichlet, about primes in arithmetic progression, which we state here without proof.

5.45 Theorem: *(Dirichlet's Theorem) For all $a, b \in \mathbb{Z}^+$ with $\gcd(a, b) = 1$, there exist infinitely many primes p with $p = a \bmod b$.*

Proof: The proof is difficult. It is usually given in PMATH 440.

5.46 Remark: Although we have not developed all of the necessary machinery to prove Dirichlet's Theorem in general, we can prove special cases of the theorem involving particular values of b. We give a few such proofs in the following example.

5.47 Example: Show that there exist infinitely many primes p of each of the following forms.
(1) $p = 1 \bmod 4$,
(2) $p = 3 \bmod 4$,
(3) $p = 1 \bmod 8$,
(4) $p = 3 \bmod 8$.

Solution: For Part 1, suppose there are only finitely many primes p with $p = 1 \bmod 4$, say $p_1, p_2, \cdots, p_\ell$ are all such primes. Let $n = (2p_1p_2 \cdots p_\ell)^2 + 1$. Let p be a prime factor of n. Note that $p \neq p_k$ for $1 \leq k \leq \ell$ because $n = 1 \bmod p_k$. Since $p \big| n$ we have $n = 0 \bmod p$, that is $(2p_1 \cdots p_\ell)^2 + 1 = 0 \bmod p$, and so $(2p_1 \cdots p_\ell)^2 = -1 \bmod p$. Thus $-1 \in Q_p$ so $p = 1 \bmod 4$. Thus we have found a prime $p = 1 \bmod 4$ which is not in the list $p_1, p_2, \cdots, p_\ell$.

For Part 2, suppose there are only finitely many primes p with $p = 3 \bmod 4$, say $p_1, p_2, \cdots, p_\ell$ are all such primes. Let $n = 4p_1p_2 \cdots p_\ell - 1$. Note that $n = -1 = 3 \bmod 4$ and note that none of the primes p_k with $1 \leq k \leq \ell$ is a factor of n because $n = -1 \bmod p_k$. The prime factors of n are odd so they are of the form $p = 1 \bmod 4$ or $p = 3 \bmod 4$. Not every prime factor of n can be of the form $p = 1 \bmod 4$, because a product of numbers of the form 1 mod 4 is also of the form 1 mod 4 but we have $n = 3 \bmod 4$. Thus n must have at least one prime factor p of the form $p = 3 \bmod 4$. Thus we have found another prime p of the form $p = 3 \bmod 4$ which is not in the list $p_1, p_2, \cdots, p_k$.

For Part 3, suppose there are only finitely many primes p with $p = 1 \bmod 8$, say $p_1, p_2, \cdots, p_\ell$ are all such primes. Let $n = (2p_1p_2 \cdots p_\ell)^4 + 1$. Let p be a prime factor of n. Since $p|n$ we have $n = 0 \bmod p$, that is $(2p_1 \cdots p_\ell)^4 + 1 = 0 \bmod p$ hence $(2p_1 \cdots p_\ell)^4 = -1 \bmod p$ and hence $(2p_1 \cdots p_\ell)^8 = 1 \bmod p$. Since $(2p_1 \cdots p_\ell)^4 = -1 \bmod p$ and $(2p_1 \cdots p_\ell)^8 = 1 \bmod p$ it follows that $\mathrm{ord}_p(2p_1 \cdots p_\ell) = 8$. Thus $8 \big| |U_p|$, that is $8 \big| (p-1)$, and so $p = 1 \bmod 8$. Thus we have found another prime p of the form $p = 1 \bmod 8$.

For Part 4, suppose there are only finitely many primes p with $p = 3 \bmod 8$, say $p_1, p_2, \cdots, p_\ell$ are all such primes. Let $n = (p_1 \cdots p_\ell)^2 + 2$. Let p be a prime factor of n. Since $p|n$ we have $n = 0 \bmod p$, that is $(p_1 \cdots p_\ell)^2 + 2 = 0 \bmod p$ hence $(p_1 \cdots p_\ell)^2 = -2 \bmod p$. Thus $-2 \in Q_p$ and so $p = 1, 3 \bmod 8$. Since each $p_k = 3 \bmod 8$ we have ${p_k}^2 = 1 \bmod 8$ so that $n = (p_1 \cdots p_\ell)^2 + 2 = 3 \bmod 8$. Not every prime factor of n can be of the form $p = 1 \bmod 8$, (because a product of numbers of the form 1 mod 8 is also equal equal to 1 mod 8) and so n must have at least one prime factor p of the form $p = 3 \bmod 8$. Thus we have found another prime $p = 3 \bmod 8$ which is not in the list $p_1, \cdots, p_\ell$.

5.48 Definition: For $x \in \mathbb{R}$, let $\pi(x) \in \mathbb{N}$ be the number of prime numbers p with $p \leq x$. For $n \in \mathbb{Z}^+$, let $p(n) = p_n \in \mathbb{Z}^+$ be the n^{th} prime number.

5.49 Remark: In section we consider theorems which describe how rapidly $\pi(x)$ and $p(n)$ tend to infinity.

5.50 Theorem: *(Bertrand's Postulate) For all $n \in \mathbb{Z}^+$ there is a prime p with $n < p \leq 2n$.*

Proof: Recall that, for a prime p and a positive integer n, $e(p, n)$ denotes the exponent of p in the prime factorization of n. Also recall that $\sum\limits_{k=0}^{n} \binom{n}{k} = 2^n$.

Claim 1: we claim that for all $n \in \mathbb{Z}^+$ we have $\prod\limits_{n<p\leq 2n} p \leq 4^n$ and $\prod\limits_{n+1<p\leq 2n+1} p \leq 4^n$, where the products are taken over prime numbers p. Let $n \in \mathbb{Z}^+$. For each prime p with $n < p \leq 2n$ we have $p \big| (2n)!$ and $p \not| \, n!$ and hence $p \big| \binom{2n}{n}$. It follows that $\prod\limits_{n<p\leq 2n} p \, \Big| \binom{2n}{n}$ and hence we have $\prod\limits_{n<p\leq 2n} p \leq \binom{2n}{n} \leq 2^{2n} = 4^n$. For each prime p with $n+1 < p \leq 2n+1$ we have $p \big| (2n+1)!$ and $p \not| \, (n+1)!$ and hence $p \Big| \binom{2n+1}{n+1}$. It follows that $\prod\limits_{n+1<p\leq 2n+1} p \leq \binom{2n+1}{n+1}$. Also note that $\binom{2n+1}{n+1} = \binom{2n+1}{n}$ so we have $2\binom{2n+1}{n+1} = \binom{2n+1}{n} + \binom{2n+1}{n+1} \leq 2^{2n+1}$ and hence $\prod\limits_{n+1\leq p\leq 2n+1} p \leq \binom{2n+1}{n+1} \leq 2^{2n} = 4^n$, as claimed.

Claim 2: we claim that $\prod\limits_{1\leq p\leq n} p \leq 4^n$ for all $n \in \mathbb{Z}^+$. Let $m \in \mathbb{Z}^+$ and suppose, inductively, that $\prod\limits_{1\leq p\leq n} p \leq 4^n$ for every integer $n < m$. When m is even, say $m = 2n$, since $\prod\limits_{1\leq p\leq n} p \leq 4^n$ by the induction hypothesis, and since $\prod\limits_{n<p\leq 2n} p \leq 4^n$ by Claim 1, it follows that $\prod\limits_{1\leq p\leq m} p = \Big(\prod\limits_{1\leq p\leq n} p\Big)\Big(\prod\limits_{n<p\leq 2n} p\Big) \leq 4^n \cdot 4^n = 4^m$. Similarly, when m is odd, say $m = 2n+1$, since $\prod\limits_{1\leq p\leq n+1} p \leq 4^{n+1}$ by the induction hypothesis, and since $\prod\limits_{n+1<p\leq 2n+1} p \leq 4^n$ by Claim 1, it follows that $\prod\limits_{1\leq p\leq m} p \leq 4^{n+1} \cdot 4^n = 4^m$. By induction, it follows that $\prod\limits_{1\leq p\leq n} p \leq 4^n$ for all $n \in \mathbb{Z}^+$, as claimed.

Claim 3: we claim that if $n \in \mathbb{Z}^+$, and p is prime with $1 \leq p \leq 2n$, and $e(p) = e\big(p, \binom{2n}{n}\big)$, then we have $p^{e(p)} \leq 2n$. Recall that $e\big(p, (2n)!\big) = \sum\limits_{k=1}^{m} \left\lfloor \frac{2n}{p^k} \right\rfloor$ and $e(p, n!) = \sum\limits_{k=1}^{m} \left\lfloor \frac{n}{p^k} \right\rfloor$ where $m = \lfloor \log_p(2n) \rfloor$ so that for $k \in \mathbb{Z}^+$ with $k > m$ we have $k > \log_p(2n)$ hence $p^k > 2n$. Verify, as an exercise, that for all $x \in \mathbb{R}$ we have $\lfloor 2x \rfloor - 2\lfloor x \rfloor \in \{0, 1\}$. It follows that

$$e(p) = e\big(p, \tbinom{2n}{n}\big) = e\big(p, (2n)!\big) - 2e\big(p, n!\big) = \sum_{k=1}^{m} \left(\left\lfloor \tfrac{2n}{p^k} \right\rfloor - 2\left\lfloor \tfrac{n}{p^k} \right\rfloor \right) \leq \sum_{k=1}^{m} 1 = m$$

and hence $p^{e(p)} \leq p^m \leq p^{\log_p(2n)} = 2n$, as claimed.

Claim 4: we claim that when $n \in \mathbb{Z}^+$, and p is a prime with $\sqrt{2n} < p \leq 2n$, and $e(p) = e\big(p, \binom{2n}{n}\big)$, then we have $e(p) \leq 1$. As in the proof of Claim 3, we have $e(p) \leq m$ where $m = \lfloor \log_p(2n) \rfloor$. Since $\sqrt{2n} < p \leq 2n$ we have $p \leq 2n$ and $p^2 > 2n$ and hence $m = 1$. Thus $e(p) \leq m = 1$, as claimed.

Claim 5: we claim that when $n \in \mathbb{Z}^+$ and p is a prime with $\frac{2}{3}n < p \leq n$, and $e(p) = e\big(p, \binom{2n}{n}\big)$ then we have $e(p) = 0$. Let $n \in \mathbb{Z}^+$ and let p be prime with $\frac{2}{3}n < p \leq n$. Multiply by 2 to get $\frac{4}{3}n < 2p \leq 2n$ and multiply by 3 to get $2n < 3p \leq 3n$. Since $p \leq n$ and $2p > \frac{4}{3}n > n$ it follows that $e\big(p, n!\big) = 1$. Since $p \leq n \leq 2n$ and $2p \leq 2n$ and $3p > 2n$ it follows that $e\big(p, (2n)!\big) = 2$. Thus $e\big(p, \binom{2n}{n}\big) = e\big(p, (2n)!\big) - 2e\big(p, n!\big) = 0$, as claimed.

Using Claims 2, 3, 4 and 5 we can now prove Bertrand's Postulate. Let $n \in \mathbb{Z}^+$ and suppose that there are no primes p with $n < p \leq 2n$. For each prime p with $1 < p \leq 2n$, write $e(p) = e\big(p, \binom{2n}{n}\big)$. Then we have

$$\begin{aligned}\binom{2n}{n} &= \prod_{1<p\leq 2n} p^{e(p)} = \prod_{1<p\leq n} p^{e(p)} \\ &= \Big(\prod_{1<p\leq\sqrt{2n}} p^{e(p)}\Big)\Big(\prod_{\sqrt{2n}<p\leq\frac{2}{3}n} p^{e(p)}\Big)\Big(\prod_{\frac{2}{3}n<p\leq n} p^{e(p)}\Big).\end{aligned}$$

By Claim 3, for all primes p with $1 < p \leq \sqrt{2n}$ we have $p^{e(p)} \leq 2n$ and so

$$\prod_{1\leq p\leq\sqrt{2n}} p^{e(p)} \leq \prod_{1\leq p\leq\sqrt{2n}} (2n) = (2n)^{\pi(\sqrt{2n})}.$$

Verify, as an exercise, that (since 2 is the only even number which is prime) we have $\pi(x) \leq \frac{x}{2}$ for all $x \geq 8$. Also verify that $\frac{\sqrt{2x}}{2} \leq \sqrt{x} - 1$ for all $x \geq 2 + \sqrt{2}$. It follows that when $n \geq 32$ so that $\sqrt{2n} \geq 8$ we have $\pi(\sqrt{2n}) \leq \frac{\sqrt{2n}}{2} \leq \sqrt{n} - 1$ and hence

$$\prod_{1\leq p\leq\sqrt{2n}} p^{e(p)} \leq (2n)^{\sqrt{n}-1}.$$

By Claim 4, for all primes p with $\sqrt{2n} < p \leq \frac{2}{3}n$ we have $e(p) \leq 1$ and, by Claim 2, we have $\prod_{1\leq p\leq\frac{2}{3}n} p^{e(p)} \leq 4^{\lfloor 2n/3\rfloor} \leq 4^{2n/3}$ and so

$$\prod_{\sqrt{2n}<p\leq\frac{2}{3}n} p^{e(p)} \leq \prod_{\sqrt{2n}<p\leq\frac{2}{3}n} p^1 \leq \prod_{1\leq p\leq\frac{2}{3}n} p \leq 4^{2n/3}.$$

By Claim 5, for all primes p with $\frac{2}{3}n < p \leq n$ we have $e(p) = 0$ so

$$\prod_{\frac{2}{3}n<p\leq n} p^{e(p)} = 1.$$

Thus

$$\binom{2n}{n} = \Big(\prod_{1<p\leq\sqrt{2n}} p^{e(p)}\Big)\Big(\prod_{\sqrt{2n}<p\leq\frac{2}{3}n} p^{e(p)}\Big)\Big(\prod_{\frac{2}{3}n<p\leq n} p^{e(p)}\Big). \leq (2n)^{\sqrt{n}-1}\cdot 4^{2n/3}\cdot 1.$$

On the other hand, since $\binom{2n}{n}$ is the largest of the binomial coefficients $\binom{2n}{k}$ and also $\binom{2n}{n} \geq 2$ we have $4^n = 2 + \sum_{k=1}^{n-1}\binom{2n}{n} \leq \binom{2n}{n} + (2n-1)\binom{2n}{n} = (2n)\binom{2n}{pn}$ so that

$$\binom{2n}{n} \geq \frac{4^n}{2n}.$$

We have shown that, at least when $n \geq 32$, we must have $\frac{4^n}{2n} \leq (2n)^{\sqrt{n}-1}\cdot 4^{2n/3}$ that is $4^{n/3} \leq (2n)^{\sqrt{n}}$. Taking the logarithm on both sides gives $\frac{n}{3}\ln 4 \leq \sqrt{n}\ln(2n)$ or equivalently $2\ln 2\sqrt{n} \leq 3\ln(2n)$. As a calculus exercise, show that for $f(x) = 3\ln(2x) - 2\ln 2\sqrt{x}$ we have $f'(x) < 0$ for $x > \frac{9}{(\ln 2)^2}$ and we have $f(154) < 0$ so that $f(x) < 0$ for all $x \geq 154$. We have shown that if there are no primes p with $n < p \leq 2n$ then we must have $n < 154$. To complete the proof, it suffices to verify that for all $n \in \mathbb{Z}^+$ with $n < 154$ there does exist a prime p with $n < p \leq 2n$.

5.51 Corollary: *For all $n \in \mathbb{Z}^+$ we have $p_n \leq 2^n$, where p_n is the n^{th} prime number.*

Proof: By Bertrand's Postulate, there is at least one prime in each of the intervals $(1,2], (2,4], (4,8], \cdots, (2^{n-1}, 2^n]$, and so there are at least n primes p with $p \leq 2^n$, and hence $p_n \leq 2^n$.

5.52 Remark: The upper bound for p_n given in the above corollary is not very tight. In fact p_n is much smaller that 2^n (see the Prime Number Therorem below).

5.53 Theorem: *Let p_n be the n^{th} prime number. Then $\sum\limits_{n=1}^{\infty} \frac{1}{p_n} = \infty$.*

Proof: Suppose, for a contradiction, that $\sum\limits_{n=1}^{\infty} \frac{1}{p_n} < \infty$. Choose $\ell \in \mathbb{Z}^+$ so that $\sum\limits_{n=\ell+1}^{\infty} \frac{1}{p_n} < \frac{1}{2}$. Let a be the product $a = p_1 p_2 \cdots p_\ell$, and consider the arithmetic progression $1+ka$, $k \in \mathbb{Z}^+$. Note that none of the primes $p_1, p_2, \cdots, p_\ell$ is a factor of any of the numbers $1+ka$, $k \in \mathbb{Z}^+$ (because for $1 \leq n \leq \ell$ we have $a = 0 \bmod p_n$ so $1+ka = 1 \bmod p_n$), so each number $1+ka$ has a prime factorization of the form $1+ka = p_{n_1} p_{n_2} \cdots p_{n_m}$ for some $n_i > \ell$ (not necessarily distinct). Notice that for each $m \in \mathbb{Z}^+$, we can expand the product

$$\Big(\sum_{n=\ell+1}^{\infty} \frac{1}{p_n} \Big)^m$$

into an infinite sum of terms of the form $\frac{1}{p_{n_1} p_{n_2} \cdots p_{n_m}}$ with each $n_i > \ell$, and each of the numbers $\frac{1}{1+ka}$ with $k \in \mathbb{Z}^+$ is equal to one of the terms in one of these sums for some m. It follows that

$$\sum_{k=1}^{\infty} \frac{1}{1+ka} \leq \sum_{m=1}^{\infty} \Big(\sum_{n=\ell+1}^{\infty} \frac{1}{p_n} \Big)^m \leq \sum_{m=1}^{\infty} \left(\tfrac{1}{2}\right)^m = 1.$$

But this is not possible since $\sum\limits_{k=1}^{\infty} \frac{1}{1+ka}$ diverges (say by the integral test).

5.54 Definition: For $f, g : \mathbb{R} \to \mathbb{R}$, we write $f(x) \sim g(x)$ when $\lim\limits_{x \to \infty} \dfrac{f(x)}{g(x)} = 1$. Similarly, for $f, g : \mathbb{Z}^+ \to \mathbb{R}$ we write $f(n) \sim g(n)$ when $\lim\limits_{n \to \infty} \dfrac{f(n)}{g(n)} = 1$.

5.55 Theorem: *(The Prime Number Theorem) Let $\pi(x)$ be the number of primes p with $p \leq x$, and let $p(n)$ be the n^{th} prime number.*
(1) We have $\pi(x) \sim \dfrac{x}{\ln x}$ *or, equivalently,* $\lim\limits_{x \to \infty} \dfrac{\pi(x) \ln x}{x} = 1$.
(2) We have $p(n) \sim n \ln n$ *or, equivalently,* $\lim\limits_{n \to \infty} \dfrac{p(n)}{n \ln n} = 1$.

Proof: The proof of this theorem is difficult. It is often given in PMATH 440. We shall only prove that Part 1 implies Part 2. Suppose that $\lim\limits_{x \to \infty} \frac{\pi(x) \ln x}{x} = 1$. Take the logarithm on both sides to get $\lim\limits_{x \to \infty} \big(\ln(\pi(x)) + \ln(\ln x) - \ln x \big) = 0$. Since $\ln x \to \infty$, we can divide by $\ln x$ to get $\lim\limits_{x \to \infty} \big(\frac{\ln(\pi(x))}{\ln x} + \frac{\ln(\ln x)}{\ln x} - 1 \big) = 0$ hence $\lim\limits_{x \to \infty} \frac{\ln(\pi(x))}{\ln x} = 1$. Since $\lim\limits_{x \to \infty} \frac{\pi(x) \ln x}{x} = 1$ it follows that $\lim\limits_{x \to \infty} \frac{\ln(\pi(x))}{\ln x} \cdot \frac{\pi(x) \ln x}{x} = 1$, that is $\lim_{x \to \infty} \frac{\pi(x) \ln(\pi(x))}{x} = 1$. Finally, by taking $x = p(n)$ so that $\pi(x) = n$, we obtain $\lim\limits_{n \to \infty} \frac{n \ln n}{p(n)} = 1$.

5.56 Example: Note that Theorem 5.53 is an immediate consequence of Part 2 of the Prime Number Theorem by the Limit Comparison Test (since $\sum\limits_{n=2}^{\infty} \frac{1}{n \ln n}$ diverges).