4.3 5. Find the prime factorization of 10!

$10! = \underline{1}\cdot\underline{2}\cdot\underline{3}\cdot 4\cdot\underline{5}\cdot 6\cdot\underline{7}\cdot 8\cdot 9\cdot 10 =$

$= 1\cdot 2\cdot 3\cdot 2\cdot 2\cdot 5\cdot 2\cdot 3\cdot 7\cdot 2\cdot 2\cdot 2\cdot 3\cdot 3\cdot 2\cdot 5 =$

$= 1\cdot 2^8\cdot 3^4\cdot 5^2\cdot 7$

11. Show that $\log_2 3$ is an irrational number.

Recall that an irrational number is a real number x that cannot be written as the ratio of two integers.

Proof by contradiction:

$\log_2 3 \rightarrow$ rational number $\frac{p}{q}$, p, q - int.

$\log_2 3 = \frac{p}{q} \iff 3 = 2^{\frac{p}{q}}$

$3^q \neq 2^p$ | by Fundamental Theorem of Arithmetics

$\log_2 3$ is irrational.

19. Show that if $2^n - 1$ is prime then n is prime.

$2^{ab} - 1 = (2^a - 1)\cdot(2^{a(b-1)} + 2^{a(b-2)} + \ldots + 2^a + 1)$.

Proof By Contradiction: Suppose n is not prime. Then n can be factored into two positive int. > 1, $n = a\cdot b$, $a, b > 1$

$$2^n - 1 = 2^{ab} - 1 = \underbrace{(2^a - 1)}_{>1}\underbrace{(2^{a(b-1)} + 2^{a(b-2)} + \ldots + 2^a + 1)}_{>1}$$

$2^n - 1$ can be factored into two factors > 1.

Therefore, $2^n - 1$ is not prime, contradicting our assumption.

Thus, n cannot be composite, it must be prime.

25. What are the greatest common divisors of these pairs of integers?

a) $3^7 \cdot 5^3 \cdot 7^3$, $2^{11} \cdot 3^5 \cdot 5^9$

$\left[gcd(a,b) = p_1^{min(a_1,b_1)} \cdot p_2^{min(a_2,b_2)} \cdots p_n^{min(a_n,b_n)} \right]$

$gcd(3^7 \cdot 5^3 \cdot 7^3, 2^{11} \cdot 3^5 \cdot 5^9) = 2^{min(11,0)} \cdot 3^{min(7,5)} \cdot 5^{min(3,9)} \cdot 7^{min(3,0)}$

$= 3^5 \cdot 5^3$

b) $11 \cdot 13 \cdot 17$, $2^9 \cdot 3^7 \cdot 5^5 \cdot 7^3$

$gcd = 1$.

c) $gcd(23^{31}, 23^{17}) = 23^{min(31,17)} = 23^{17}$.

d) $gcd(41 \cdot 43 \cdot 53, 41 \cdot 43 \cdot 53) = 41 \cdot 43 \cdot 53$

e) $gcd(3^{13} \cdot 5^{17}, 2^{12} \cdot 7^{21}) = 1$

f) $gcd(1111, 0) = 1111$

37. Use ex36 to show that if a and b are positive integers, then $gcd(2^a-1, 2^b-1) = 2^{gcd(a,b)} - 1$.

$\left[(2^a-1) \bmod (2^b-1) = 2^{a \bmod b} - 1 \right]$

Proof:

Using the Euclidean Algorithm:

$gcd(a,b) = gcd(b, a \bmod b)$

From ex36: $(2^a-1) \bmod (2^b-1) = 2^{a \bmod b} - 1 \Rightarrow$

Let's denote $r = a \bmod b$:

$gcd(2^a-1, 2^b-1) = gcd(2^{a \bmod b}-1, 2^b-1)$

$gcd(2^b-1, 2^r-1) = gcd(2^r-1, 2^{b \bmod r}-1)$

...

$gcd(2^{gcd(a,b)}-1, 2^{gcd(a,b)}-1) \Rightarrow 2^{gcd(a,b)}-1$

$gcd(2^a-1, 2^b-1) = 2^{gcd(a,b)} - 1$.